SCREEN MY BONES – PRIVACY POLICY

This privacy policy applies to Screen My Bones Ltd (**we**, **us** or **our**). We are committed to protecting your privacy. This policy explains how we collect, use and share your personal data. It applies to all personal data we handle, whether we collect it through our website, in person, or through other means. This privacy policy takes into account the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as well as the Privacy Act 1988 (Cth) and the Australian Privacy Principles for Australian residents, and applicable US federal and state privacy laws for US residents.
In addition:

- Individuals located in Australia may have rights under the Privacy Act 1988 (Cth) and the Australian Privacy Principles. Annexure 1 outlines additional rights and information for Australian residents.
- Individuals located in the United States of America or any of its territories may have additional rights under federal or state laws. Annexure 2 outlines additional rights and information for US residents.

Information we collect

Identity and contact details

- Name, address, email address and phone number
- Professional details Service related information
- Transaction details for products and services you've purchased from us or enquiries about our products and services
- Your preferences for our services and your marketing preferences and where relevant information related to loyalty programmes
- Feedback, complaints and compliments and survey responses Financial and payment information
- Payment details for products and services you've purchased from us (including where relevant, credit reference information) and where relevant banking or payment card information

Digital information

- IP address and general location information derived from your IP address
- Search and browsing behaviour and user journeys
- Website usage patterns
- Cookie preferences and tracking Recordings
- Call recordings
- Records of meetings and decisions Professional information (for job applicants and workers)
- Employment history
- Professional experience
- Required authorisations and licences
- Professional registrations
- Information about your right to work in the UK Special category data

This is special information that the law says is more sensitive (sometimes called “sensitive personal data”). We handle special category data with extra care and protection, and we only collect and use these where legally permitted. This includes:

- Racial or ethnic origin

- Health information (including dietary requirements, allergies and health conditions)

How we collect personal data

- **Directly from you when you:** when you interact with us, contact us, fill out forms.
- **Automatically when you:** visit our website, use our technologies, interact with our online services.
- **From third parties:** service providers, business partners, previous employers, government organisations and organisations or people authorised by you.
- **From publicly available sources:** such as Companies House and professional networking sites such as LinkedIn.

How we use your information

Data protection law requires us to have proper legal reasons for using your personal data. We can only use your information when we have one or more of these legal bases.

- **Consent** - You have clearly agreed to us using your personal data for a specific purpose.
- **Performance of a contract** - We need to use your information to fulfil a contract with you, or because you've asked us to do something before entering into a contract.
- **Legal duty** - We must use your information to comply with the law.
- **Vital interests** - We need to use your information to protect someone's life.
- **Public interest** - We need to use your information to perform a task in the public interest or carry out official functions that have a clear legal basis.
- **Legitimate interests** - We have a genuine business reason to use your information, or a third party does, but only if this doesn't unfairly override your rights and interests. Where we rely on legitimate interests as our legal basis, we have conducted balancing tests to ensure our interests do not override your fundamental rights and freedoms. These assessments consider:
    - The nature of our legitimate interest
    - The impact on you
    - Any safeguards we can implement

- Your reasonable expectations
- The broader context of our relationship

Note that we may process your personal data for more than one legal basis depending on the specific purpose for which we are using your data. We have listed the reasons we process your data and the legal basis below. Please reach out to us if you need further details about the specific legal basis we are relying on to process your personal data.

Managing your account and providing our services

What we use your information for:

- To enable you to access and use our software, including providing login credentials
- To provide our services to you, including dispatch and delivery of products, event registration, appointment management
- To contact and communicate with you about our services, including responding to support requests and enquiries and for dealing with complaints or claims
- Internal record keeping, administrative, invoicing and billing purposes Legal basis for using this information:
- Performance of a Contract
- Legal Duty (for billing and record-keeping requirements)
- Legitimate interests
- Consent

Types of information we use:

- Identity and contact details
- Service related information
- Financial Information
- Digital information
- Special categories of personal data

Client onboarding and verification

What we use your information for:

- To assess whether to take you on as a new client, including performing anti-money laundering, anti-terrorism, sanction screening, fraud and other background checks

Legal basis for using this information:

- Performance of a Contract
- Legal Duty
- Public Interest
- Legitimate interests Types of information we use:
- Identity and contact details
- Financial information

Website enquiries and customer service

What we use your information for:

- To contact and communicate with you about any enquiries you make with us via our website Legal basis for using this information:
- Legitimate interests Types of information we use:
- Identity and Contact Data
- Digital Information

Business improvement and development

What we use your information for:

- Analytics including profiling on our website
- Market research and business development
- To operate and improve our services, associated applications and associated social media platforms Legal basis for using this information:
- Legitimate interests Types of information we use:
- Digital Information **Marketing and communications** What we use your information for:
- To send you promotional information about our events and experiences and information that we consider may be of interest to you
- To run promotions, competitions and offer additional benefits to you Legal basis for using this information:
- Legitimate interests Types of information we use:
- Identity and Contact Data
- Digital Information **Recruitment and employment purposes** What we use your information for:
- To consider your application if you have applied to work with us and to keep you up to date with its progress
- In relation to self-declared disabilities in order for us to make a reasonable adjustments to support your application and any possible future employment

- In relation to any diversity or equal opportunities monitoring questionnaire data, to monitor and report on our equality and diversity composition and ensure fairness in the recruitment process
- In relation to any right to work information we collect, in order to ensure we comply with the law in employing you
- To keep you updated on any other suitable vacancies Legal basis for using this information:
- Legitimate interests
- Legal Duty
- Consent
- Performance of a Contract Types of information we use:
- Identity and Contact Data
- Professional Data

Legal compliance

What we use your information for:

- Comply with our legal obligations or if otherwise required or authorised by law Legal basis for using this information:
- Legal Duty

Types of information we use:

- All relevant Personal Data

Our disclosures of personal data to third parties

We may disclose personal data to:

Service providers

- IT service providers including Microsoft Office and Microsoft Azure
- Data storage providers
- Web hosting and server providers
- Payment processors including Stripe
- Marketing and advertising providers
- Analytics providers

Professional advisers

- Bankers
- Auditors
- Insurers and insurance brokers
- Legal advisers

Business partners

- Our existing or potential agents
- Our business partners or contractors

Corporate transactions

If we merge with or are acquired by another company, or sell our business assets:

- Your information may be disclosed to our advisers
- Your information may be disclosed to the potential purchaser's advisers
- Your information may be included in the transferred assets

Legal and regulatory bodies

- Courts and tribunals
- Regulatory authorities including as required for reporting obligations
- Law enforcement officers

Other parties

- Third parties you have authorised
- Emergency services when necessary
- Any other parties as required or permitted by law

Overseas transfers

Where we store and access your information

We store your personal data in the United Kingdom. However, your information may be transferred to locations outside the United Kingdom in these circumstances:

- When our service providers are located overseas
- When we work with overseas business partners
- When using cloud-based services or data storage solutions
- When required by law or legal proceedings

Our approach to overseas transfers

When we transfer your personal data outside the United Kingdom, we ensure it receives appropriate protection by:

- Only transferring your information to countries that UK data protection law recognises as providing adequate protection for personal data, or
- Putting in place a contract with the third party that means they must protect personal data to the same standards as the UK.
- Transferring personal data to organisations that are part of specific agreements on cross-border data transfers with the UK.

What this means for you

We only transfer the minimum amount of personal data necessary and require all recipients to:

- Protect your information to the same standards required by UK law
- Use your information only for the purposes we've agreed
- Allow us to monitor how they handle your information
- Provide you with the same rights over your information that you have under UK law

Children's Personal Data

We do not knowingly collect or process personal data from children under 13 years of age without appropriate parental or guardian consent.

If you are under 13, please do not provide personal data to us without first asking your parent or guardian for permission.
If we become aware that we have collected personal data from a child under 13 without verified parental consent, we will take steps to delete that information as quickly as possible.

Parents and guardians have the right to:

- Review any personal data we hold about their child
- Request correction or deletion of their child's personal data
- Refuse or withdraw consent for further collection or use of their child's data
- Contact us with any concerns about their child's privacy

If you are a parent or guardian and believe your child has provided us with personal data without your consent, please contact us immediately using the details provided in this policy.

Data retention

How long we keep your information

We only keep your personal data for as long as we need it to:

- Provide our services to you
- Meet our legal, tax, accounting or regulatory obligations
- Handle any complaints or legal issues that may arise We may keep your information for longer periods if:
- You make a complaint that we need to investigate or respond to
- We reasonably believe legal action involving our relationship with you might occur
- The law requires us to keep it for specific timeframes

How we decide retention periods

When determining how long to keep your information, we consider:

- How much information we have and how sensitive it is
- The risk of harm if the information was accessed without permission
- Whether we can achieve our purposes in other ways
- What legal, regulatory, tax or accounting rules require
- The nature of our relationship with you and the services we provide

What happens when we no longer need your information

Once we no longer need your personal data, we will securely delete or destroy it in accordance with our data retention policies and legal requirements.

Your Rights

You can request information about retention periods for your data and ask for early deletion where legally possible.

Your privacy rights and choices

Providing information

You can choose whether to provide personal data to us, however, if you don't provide certain information, we may not be able to provide some services. Let us know if you don't want to provide information and we will let you know when information is required versus optional.

Right of Access

You have the right to ask us for copies of your personal data. You can request other information such as details about where we get personal data from and who we share personal data with. There are some exemptions which means you may not receive all the information you ask for.

Right to Rectification

You have the right to ask us to correct or delete personal data you think is inaccurate or incomplete.
Right to Erasure (“Right to be forgotten”)
You can request deletion of your personal data in certain limited circumstances as set out in data protection law, such as where the data is no longer necessary or has been unlawfully processed. This right is not absolute and we may be required or entitled to retain your data for legal, regulatory or legitimate business reasons.
Right to Restrict Processing
You can ask us to suspend processing where:

- You contest the accuracy of the data
- Processing is unlawful but you don't want erasure
- We no longer need the data but you need it for legal claims
- You've objected to processing pending verification of our legitimate grounds

Right to opt-out of marketing communications
You can opt-out of receiving marketing communications at any time. Each marketing communication will include an unsubscribe option. You can change your marketing preferences by contacting us. We will process your request as soon as practicable.
Right to Data Portability
Where technically feasible, you can receive your personal data in a structured, commonly used format or have it transmitted to another controller where:

- Processing is based on consent or contract
- Processing is automated

Right to Object
You can object to processing based on legitimate interests or for direct marketing purposes. We will stop processing unless we can demonstrate compelling legitimate grounds.
Right to Withdraw Consent
Where processing is based on consent, you can withdraw it at any time without affecting the lawfulness of prior processing.
How to Exercise Your Rights
To exercise any of these rights, contact us using the details below. We may ask for proof of identity and will respond within one month (extendable to three months for complex requests).
These rights are available under data protection law, though some may not apply in every situation. We'll let you know if any limitations apply when you make a request.
Making a complaint
If you have concerns about how we handle your information.
If you're unhappy with how we've used your personal data, please get in touch with us first using the contact details at the end of this policy. When you contact us:

- Give us full details about your complaint
- We'll investigate your concerns promptly
- We'll respond to you in writing explaining what we found and what we'll do to address your complaint Your right to complain to the regulator

You can also make a complaint directly to the Information Commissioner's Office (ICO), the UK's data protection regulator, at any time.

The ICO’s address:
Information Commissioner’s Office Wycliffe House
Water Lane

Wilmslow Cheshire SK9 5AF
Helpline number: 0303 123 1113
Website: https://www.ico.org.uk/make-a-complaint
You don't have to contact us first before going to the ICO, but we'd appreciate the opportunity to try to resolve your concerns directly with you.
Protecting your information
We use multiple layers of security to protect your information.
Technical safeguards

- Enterprise-grade encryption for data storage and transmission
- Regular security testing and monitoring
- Automated threat detection systems

Operational security

- Staff training on security and privacy
- Strict access controls based on job requirements
- Regular security audits and incident response procedures testing

Physical security

- Secure premises with controlled access
- Secure disposal of physical documents
- Equipment security protocols

Public information
Please note that any information you choose to share publicly on online platforms (such as comments or reviews) can be accessed and used by others. We cannot control or protect information that you make publicly available.

Cookies and analytics

Cookies and pixels
We use cookies and similar tracking technologies on our website to enhance your browsing experience and improve our services.
What are cookies?
Cookies are small text files that are stored on your device when you visit our website. They help us remember your preferences and understand how you use our site.
Types of cookies we use

- Essential cookies: Necessary for the website to function properly
- Performance cookies: Help us understand how visitors interact with our website
- Functionality cookies: Remember your preferences and settings
- Marketing cookies: Used to deliver relevant advertisements and track campaign effectiveness Cookie consent

When you first visit our website, you will see a cookie notice explaining our use of cookies. You can choose which types of cookies to accept through our cookie preference centre. You'll find more information about the cookies we use in our cookie pop-up.

Managing your preferences
You can change your cookie preferences at any time by:

- Using our cookie preference centre on the website
- Adjusting your browser settings to refuse or delete cookies
- Visiting our cookie policy for detailed information about specific cookies

Please note that disabling certain cookies may affect the functionality of our website and your user experience.
Google Analytics
We use Google Analytics to understand how people use our website. This involves cookies that collect information about your browsing activity. You can opt out of Google's advertising features through your Google account settings, browser add-ons, or your device's privacy settings. Google provides various tools and options to control how your data is used for advertising purposes. You can learn more about how Google uses your data and your available options on Google's privacy pages.
Meta advertising tools
We use Meta's advertising tools (such as Meta Pixel) to understand how our ads perform and to show you more relevant advertisements on Meta platforms like Facebook and Instagram when you visit our website or app. You can manage whether we connect information from our website with your Meta account for advertising purposes by adjusting your settings within your Meta account preferences.
Microsoft Clarity
We use Microsoft Clarity to understand how visitors use our web application through behavioural metrics, heatmaps and session replay. Clarity only operates after you accept analytics cookies, and is configured in strict masking mode so that personal and health information is hidden before any recording leaves your browser. Microsoft processes this information in accordance with the Microsoft Privacy Statement (https://privacy.microsoft.com/privacystatement). You can withdraw your consent at any time through our cookie preference centre.

Use of location services data

We collect your precise or approximate location via our web application for the following purposes:

- To provide geographically relevant scan location recommendations based on your postcode
- To generate demographic analytics to improve our service coverage and accessibility
- To direct inquiries to appropriate local scanning centres
- To enhance user experience by providing location-specific information and educational content
- For security and safety
- To prevent and detect fraud
- As permitted by law

We collect this information when you work with us. If you do not want us to use your location for the purposes above, you should turn off the location services in your mobile phone settings. If you do not provide geolocation data to us, it may affect our ability to work with you as a customer or supplier of our business.

Artificial Intelligence (AI) Technologies

Overview
We use artificial intelligence and machine learning technologies in our business operations and services, including AI tools provided by third parties. We only use these technologies when legally permitted and necessary for our business.
How we use AI

We may use AI technologies to:

- Conduct analysis and data processing
- Generate and modify content and coding
- Improve and optimise our services and operations
- Automate routine tasks and communications
- Personalise your experience with our services
- Support quality assurance processes
- Assist with customer support and queries

Data protection and security

- When we work with third-party AI providers, we ensure they handle your personal data in accordance with privacy laws through contractual requirements and appropriate safeguards.

Your rights and our commitments

- Any information generated or inferred about you by AI technologies is treated as personal data, and you maintain all the rights outlined in this privacy policy. When using AI with your personal data, we commit to:

Transparency and control

- We'll inform you when AI is used to make decisions that may significantly affect you
- We maintain human oversight and review of significant AI-generated decisions
- Our staff are trained to understand AI limitations and verify outputs before relying on them
- We implement processes to verify the accuracy of AI-generated outputs

Security

- We use appropriate technical and organisational measures to maintain the security and integrity of your personal data
- We regularly test and monitor AI outputs for accuracy and reliability

Risk mitigation

- We regularly assess and document risks associated with using AI to process personal data
- We implement appropriate measures to address these risks
- We continuously monitor AI performance and regularly review their impact

Amendments

We may update this policy at any time by posting the revised version on our website. We recommend that you review our website regularly to stay current with any policy changes.

Our contact details

Privacy contact email: info@screenmybones.com

Last update: 19 March 2026

© LegalVision Law UK Ltd

ANNEXURE 1: ADDITIONAL RIGHTS AND INFORMATION FOR INDIVIDUALS LOCATED IN AUSTRALIA

This Annexure 1 sets out additional rights and information for individuals located in Australia under the Privacy Act 1988 (Cth) and the Australian Privacy Principles.

Sensitive Information

Under Australian privacy law, sensitive information is a sub-set of personal information that is given a higher level of protection. Sensitive information means information relating to your racial or ethnic origin, political opinions, religion, trade union or other professional associations or memberships, philosophical beliefs, sexual orientation or practices, criminal records, health information or biometric information. The type of sensitive information that we might collect about you includes your health information when you use our services.

Collection from Third Parties

If we receive personal information about you from a third party, we will protect it as set out in this privacy policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such person's consent to provide the personal information to us.

Your Choice

Please read this privacy policy carefully. If you provide personal information to us, you understand we will collect, hold, use and disclose your personal information in accordance with this privacy policy. You do not have to provide personal information to us, however, if you do not, it may affect our ability to do business with you.

Access to Personal Information

You may request access to the personal information that we hold about you. An administrative fee may be payable for the provision of such information.
Please note, in some situations, we may be legally permitted to withhold access to your personal information. If we cannot provide access to your information, we will advise you as soon as reasonably possible and provide you with the reasons for our refusal and any mechanism available to complain about the refusal.
If we can provide access to your information in another form that still meets your needs, then we will take reasonable steps to give you such access.

Correction of Personal Information

If you believe that any information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, please contact us using the details below. We will take reasonable steps to promptly correct any information found to be inaccurate, out of date, incomplete, irrelevant or misleading.
Please note, in some situations, we may be legally permitted to not correct your personal information. If we cannot correct your information, we will advise you as soon as reasonably possible and provide you with the reasons for our refusal and any mechanism available to complain about the refusal.

Overseas Transfers

We store your personal information in the United Kingdom. Where we disclose your personal information to third parties, those third parties may store, transfer or access personal information outside of Australia. We will only disclose your personal information overseas in accordance with the Australian Privacy Principles.

Notifiable Data Breaches Scheme

We comply with the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth). If we suspect or become aware of an eligible data breach involving your personal information that is likely to result in serious harm to you, we will:

- Conduct an assessment to determine if the breach is likely to result in serious harm
- Notify you and the Office of the Australian Information Commissioner as soon as practicable if we determine that serious harm is likely
- Include in our notification a description of the breach, the kind of information concerned, and recommendations about steps you should take in response

Australian Privacy Principles Compliance

We handle your personal information in accordance with the Australian Privacy Principles, which require us to:

- Be open and transparent about how we manage personal information (APP 1)
- Give you the option of not identifying yourself or using a pseudonym where practicable (APP 2)
- Only collect personal information that is reasonably necessary for our functions or activities (APP 3)
- Collect personal information directly from you where reasonable and practicable (APP 3)
- Notify you of certain matters when we collect your personal information (APP 5)
- Only use or disclose your personal information for the primary purpose for which it was collected, or a secondary purpose where you would reasonably expect us to, or where you have consented (APP 6)
- Take reasonable steps to ensure personal information we use or disclose is accurate, up-to-date, complete and relevant (APP 10)
- Take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure (APP 11)

Direct Marketing

We may only use or disclose your personal information for direct marketing purposes if:

- We collected the information from you and you would reasonably expect us to use or disclose it for direct marketing
- We collected the information from you, you would not reasonably expect us to use it for direct marketing, but you have consented or it is impracticable to obtain your consent
- We collected the information from a third party and you have consented or it is impracticable to obtain your consent

You may opt out of direct marketing at any time by using the unsubscribe facility in our marketing communications or by contacting us.

Government Related Identifiers

We will not use or disclose a government related identifier (such as a Medicare number or driver's licence number) unless:

- The use or disclosure is reasonably necessary to verify your identity
- The use or disclosure is reasonably necessary for us to fulfil our obligations to a government agency

- The use or disclosure is required or authorised by law
- A permitted general situation exists
- We reasonably believe the use or disclosure is reasonably necessary for one or more enforcement related activities

Contact for Australian Privacy Matters

For any questions or notices relating to Australian privacy matters, or would like to make a complaint, please contact us at: info@screenmybones.com

Making a Complaint

If you are an Australian resident and are not satisfied with our response to your complaint, you may contact the Office of the Australian Information Commissioner:
Website: https://www.oaic.gov.au/ Phone: 1300 363 992
Email: enquiries@oaic.gov.au

ANNEXURE 1: ADDITIONAL RIGHTS AND INFORMATION FOR INDIVIDUALS LOCATED IN UNITED STATES OF AMERICA

This Annexure 2 sets out additional rights and information for individuals located in the United States of America under applicable US federal and state privacy laws.

HIPAA and Health Information

To the extent we create, receive, maintain, or transmit protected health information ("PHI") on behalf of a covered entity or another business associate, we do so solely in our capacity as a business associate and in accordance with applicable US health information privacy and security laws, including the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA").
Use and Disclosure of PHI:

- We use and disclose PHI only as permitted by our applicable business associate agreements and as required by law
- We do not use PHI for our own marketing or commercial purposes Security Safeguards:
- We maintain administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of PHI, consistent with HIPAA requirements and industry standards

Individual Rights:

- Individuals' rights with respect to PHI (including rights of access, amendment, and accounting of disclosures) are administered by the applicable covered entity
- Requests relating to PHI should be directed to the relevant covered entity or health plan Service Provider Role:
- When we process personal information, including health-related information, on behalf of our customers, we do so as a service provider or processor and strictly in accordance with the customer's instructions and applicable agreements

California Privacy Rights

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).
Additional Rights:

In addition to the rights set out in our privacy policy, California residents can request to:

- Deletion: Have your personal information deleted (to the extent permitted by law), which may impact your ability to use our website or our services
- Opt-Out of Sale or Sharing: Opt out of the sale of your personal information (although please note that we do not sell your personal information) or sharing of your personal information for cross-context behavioural advertising. You may also use the 'Global Privacy Control' signal to exercise this right
- Limit Use of Sensitive Information: Ask that we limit our use and disclosure of your sensitive personal information to certain purposes permitted by law
- Authorised Agent: Have an authorised agent make requests on your behalf Non-Discrimination:

We will not discriminate against you for exercising your rights, nor will we:

- Deny you access to our services

- Charge different prices
- Provide a different level of service
- Suggest that any of those things might occur if you exercise your rights 'Shine the Light' Law:

California residents have a right under section 1798.83 of the California Civil Code to request details about the personal information that we have shared with third parties for their direct marketing purposes, and who those third parties are.
California residents who would like to make a request for this notice can do so by contacting us through the email address set out at the end of this privacy policy. Please include your full name and postal address in your email so that we can verify your residency in California and respond.
Categories of Personal Information:

For California residents, the categories of personal information we collect are described in the "Information we collect" section of the privacy policy above. We collect these categories for the business purposes described in the "How we use your information" section.
No Sale of Personal Information:

We do not sell your personal information and have not sold personal information in the preceding 12 months.

Other State Privacy Rights

Residents in other states (including Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Nevada, Oregon, Texas, Utah and Virginia) may have additional rights under state law.
Your Rights May Include:

- Access: Request access to your personal information
- Deletion: Request deletion of your personal information
- Correction: Request correction of your personal information
- Opt-Out of Targeted Advertising: Opt out of the processing of your personal information for the purposes of targeted advertising
- Opt-Out of Sale: Opt out of the sale of your personal information (although please note that we do not sell your personal information)
- Data Portability: In some states, request a copy of your personal information in a portable format Authorised Agents:

You may use an authorised agent to submit a request to opt out of targeted advertising or the sale of personal data (although please note that we do not sell your personal information).

Authorised agents may submit such requests to the email address set out at the end of this privacy policy, provided that we have been given verification of your identity and confirmation that you provided the agent with authority to act on your behalf.
Appeals Process:

If we decline to take action on your request, you may appeal our decision by contacting us using the details below. We will respond to your appeal within the timeframe required by applicable state law.

Children's Privacy Under US Law

We comply with the Children's Online Privacy Protection Act (COPPA) and do not knowingly collect personal information from children under 13 years of age without verifiable parental consent.

If you are a parent or guardian and believe your child under 13 has provided us with personal information without your consent, please contact us immediately using the details provided in this policy, and we will take steps to delete that information as quickly as possible.

Do Not Track Signals

Some web browsers have a "Do Not Track" feature. Currently, we do not respond to "Do Not Track" signals, except where required by applicable state law (such as the Global Privacy Control for California residents).

Contact for US Privacy Matters

For any questions or notices relating to US privacy matters, or to exercise your rights under US privacy laws, please contact us at: Email: info@screenmybones.com

Making a Complaint

If you are a US resident, you may also have the right to lodge a complaint with your state's Attorney General or relevant data protection authority depending on your state of residence.