MOMENTUM TRACKING — PRIVACY POLICY

Effective Date: June 2025
Last Updated: [Insert Date]
Jurisdiction: Victoria, Australia

1. OVERVIEW

1.1 This Privacy Policy explains how Momentum Tracking handles personal information and sensitive information in connection with the App.

1.2 We aim to handle information in accordance with applicable Australian privacy laws, including the Privacy Act 1988 (Cth), the Australian Privacy Principles, and the Notifiable Data Breaches scheme where those laws apply.

1.3 The Australian Privacy Principles set out standards, rights, and obligations for handling personal information, and the NDB scheme requires notification to affected individuals and the OAIC where an eligible data breach is likely to result in serious harm.

1.4 Because the App may be used by fitness professionals to store health-related client information, users should also consider any obligations that apply to health information, including Victorian health-records laws where relevant. The Health Records Act 2001 (Vic) is in force in Victoria.

1.5 This Privacy Policy should be read together with our Terms of Service.

2. INFORMATION WE COLLECT

2.1 We collect information that you choose to enter, upload, generate, store, or manage through the App.

2.2 This may include business information such as your business name, ABN, contact details, pricing, packages, revenue records, invoices, expenses, reports, and account settings.

2.3 This may include client information such as names, contact details, session history, package balances, payment status, notes, forms, goals, attendance history, and related records.

2.4 This may include financial and business tracking information such as income, payments, debts, outstanding invoices, expenses, GST estimates, BAS-related summaries, PAYG-related estimates, and revenue projections.

2.5 This may include sensitive or health-related information such as PAR-Q responses, injuries, medical history disclosed by clients, exercise limitations, health screening notes, or other health-related client information.

2.6 We may collect technical information necessary to operate the App, such as account identifiers, device information, browser information, log data, usage events, diagnostic data, error reports, and security-related records.

2.7 Payment information may be collected and processed by third-party payment providers such as Stripe. We do not generally store full card details ourselves.

3. HOW INFORMATION IS COLLECTED

3.1 Information is collected when you enter it into the App, create an account, enable cloud sync, use features, generate reports, contact support, subscribe to a paid plan, or interact with the website or App.

3.2 Some information may be collected automatically through browser storage, cookies, analytics tools, logs, security tools, or infrastructure services.

3.3 We aim to collect only information reasonably necessary to operate, support, maintain, secure, improve, and provide the App.

3.4 You must not enter information about another person unless you have the right, authority, consent, or lawful basis to do so.

4. YOUR ROLE AS USER

4.1 You control the information you enter into the App.

4.2 You are responsible for deciding what personal information and sensitive information is collected from your clients.

4.3 You are responsible for explaining your own privacy practices to your clients.

4.4 You are responsible for obtaining client consent before collecting or storing personal information, sensitive information, or health information.

4.5 You are responsible for responding to client requests relating to access, correction, deletion, complaints, or privacy concerns where those requests relate to data you entered into the App.

4.6 Momentum Tracking acts as a software platform provider. We do not independently determine your client privacy obligations, consent requirements, professional obligations, or data-retention requirements.

5. PURPOSES OF USE

5.1 We use information to provide and operate the App.

5.2 We may use information to create and maintain accounts, store and display records, enable cloud sync, process payments, generate reports, export data, troubleshoot issues, respond to support requests, improve features, prevent misuse, maintain security, and comply with law.

5.3 We may use de-identified, aggregated, or anonymised information to understand usage patterns, improve the App, diagnose issues, develop features, and improve performance.

5.4 We do not sell personal information to advertisers or data brokers.

5.5 We do not use your client health information for advertising.

6. SENSITIVE AND HEALTH INFORMATION

6.1 Sensitive information, including health information, requires a higher level of care.

6.2 You must obtain explicit consent before entering health information into the App.

6.3 You must only enter health information that is reasonably necessary for your legitimate business, training, screening, or client-management purposes.

6.4 You must ensure that health information is accurate, relevant, current, secure, and not excessive.

6.5 You must not use the App to store emergency medical records, urgent clinical information, or information that should be held in a dedicated medical or clinical system.

6.6 We do not provide clinical, medical, diagnostic, treatment, rehabilitation, or allied health services through the App.

6.7 We do not review health information for accuracy, risk, red flags, medical suitability, or safety.

7. DATA STORAGE AND LOCATION

7.1 Information may be stored locally in your browser.

7.2 If cloud sync is enabled, information may be stored using cloud infrastructure, including Supabase or other providers.

7.3 Third-party providers may store or process information in Australia or overseas depending on their infrastructure, policies, configuration, and service arrangements.

7.4 You acknowledge that cloud services may involve cross-border storage, processing, support, redundancy, backups, or technical access.

7.5 We take reasonable steps to work with reputable providers, but we do not control every aspect of third-party infrastructure.

7.6 You are responsible for deciding whether cloud storage is appropriate for the type of information you choose to enter.

8. SECURITY

8.1 We take reasonable technical and organisational steps to protect information handled through the App.

8.2 Security measures may include access controls, authentication systems, third-party infrastructure security, database rules, monitoring, backups, encryption features where available, and operational safeguards.

8.3 No system is completely secure. We cannot guarantee that unauthorised access, disclosure, loss, corruption, misuse, or interference will never occur.

8.4 Your security practices are critical. You are responsible for securing your devices, browsers, passwords, email accounts, payment accounts, and account access.

8.5 You should avoid using shared devices, public computers, insecure networks, weak passwords, or untrusted browser extensions when handling client or business data.

8.6 You must notify us promptly if you suspect unauthorised access, compromise, or a security incident affecting your account or data.

9. DATA RETENTION

9.1 Local data may remain in your browser until you delete it, clear browser storage, uninstall or reset your browser, change devices, or otherwise remove it.

9.2 Cloud data may remain until you delete it, close your account, request deletion, or until it is removed according to our operational practices.

9.3 We may retain some information where reasonably necessary for legal, accounting, tax, security, fraud prevention, backup, dispute-resolution, or legitimate business purposes.

9.4 Backup copies may persist for a limited period after deletion due to technical and operational processes.

9.5 You are responsible for exporting data before deleting your account, clearing local data, cancelling your subscription, or ending use of the App.

10. ACCESS, CORRECTION AND DELETION

10.1 You may access, correct, export, or delete much of your data using App features where available.

10.2 You may request assistance with access, correction, export, or deletion by contacting support.

10.3 We may need to verify your identity before responding to requests.

10.4 We may refuse or limit requests where permitted by law, including where the request is unreasonable, unlawful, technically impossible, impacts another person's privacy, affects legal obligations, or relates to data controlled by you rather than us.

10.5 If your clients request access, correction, or deletion of information you entered into the App, you are generally responsible for responding to that request as the business that collected the information.

11. DISCLOSURE OF INFORMATION

11.1 We may disclose information to service providers who help us operate the App, including cloud hosting, database, payment, email, analytics, customer support, security, and infrastructure providers.

11.2 We may disclose information where required by law, regulation, court order, government request, enforcement process, or legal obligation.

11.3 We may disclose information where reasonably necessary to protect our rights, users, systems, security, business, legal position, or the safety of others.

11.4 We may disclose information in connection with a business sale, merger, acquisition, restructure, financing, asset sale, or transfer of the App, provided reasonable confidentiality protections apply.

11.5 We do not sell client information or health information to advertisers.

12. THIRD-PARTY SERVICES

12.1 The App may use Supabase, Netlify, Stripe, and other providers.

12.2 These providers may collect, store, process, transmit, or access information as necessary to provide their services.

12.3 Their handling of information is governed by their own privacy policies, terms, and security practices.

12.4 We recommend reviewing the privacy policies of relevant third-party providers.

12.5 We are not responsible for third-party privacy practices except to the extent required by law.

13. NOTIFIABLE DATA BREACHES

13.1 We take data breaches seriously.

13.2 If we become aware of a suspected data breach, we will take reasonable steps to assess the incident.

13.3 Where the Notifiable Data Breaches scheme applies and an eligible data breach has occurred, we will notify affected individuals and the OAIC where required.

13.4 The OAIC explains that an eligible data breach generally involves unauthorised access, unauthorised disclosure, or loss of personal information that is likely to result in serious harm.

13.5 If a breach relates to your account, device, browser, credentials, staff, contractors, or business practices, you may also have obligations to notify affected individuals, regulators, clients, insurers, or other parties.

14. CHILDREN'S PRIVACY

14.1 The App is intended for use by adults and business operators aged 18 or over.

14.2 The App is not intended to be used directly by children.

14.3 If you store information about minors, you are responsible for ensuring you have the legal right, parent or guardian consent where required, and appropriate privacy disclosures.

14.4 You must take additional care when handling information about minors.

15. MARKETING COMMUNICATIONS

15.1 We may send you service messages, account messages, security notices, billing notices, legal notices, and important App updates.

15.2 We may send marketing emails where permitted by law.

15.3 You may unsubscribe from marketing communications, but you may still receive important service or account-related messages.

16. INTERNATIONAL USERS

16.1 The App is operated from Australia and primarily intended for Australian users.

16.2 If you access the App from outside Australia, you are responsible for ensuring your use complies with local laws.

16.3 You acknowledge that information may be processed in Australia or other countries depending on the providers used.

17. CHANGES TO THIS PRIVACY POLICY

17.1 We may update this Privacy Policy from time to time.

17.2 Updated versions may be posted on the website, shown in the App, or otherwise made available.

17.3 Continued use of the App after changes indicates acceptance of the updated Privacy Policy.

18. COMPLAINTS

18.1 If you have a privacy complaint, contact us first at support@momentumtracking.com.au.

18.2 We will aim to respond within a reasonable time.

18.3 If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner.

19. CONTACT

Momentum Tracking

[Insert Legal Entity Name]

ABN: [Insert ABN]

Website: momentumtracking.com.au

Email: support@momentumtracking.com.au