Frank Partners Pty Ltd - Privacy Policy

Last updated: 2 February 2026

1. Introduction

Frank Partners Pty Ltd ("we", "us", "our", or "Frank Partners") is committed to protecting the privacy of your personal information. We understand that how we collect, use, store, and share your personal information is important to you, and we take that responsibility seriously.

This privacy statement explains our privacy practices in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth). It describes the types of personal information we collect, how we use and disclose that information, how we protect it, and what rights you have in relation to your information.

If you have any questions about this privacy statement or our privacy practices, please contact us using the details provided in Section 12 of this statement.

2. About Frank Partners

Frank Partners is a management consulting firm based in Melbourne, Victoria. We provide strategic advisory services, transformation support, technology implementation guidance, and organisational change consulting to clients across public and private sectors in Australia.

This privacy statement applies to all of Frank Partners' functions and activities, including our consulting engagements, business development activities, website operations, and internal business management.

3. Types of Personal Information We Collect and Hold

We collect and hold personal information necessary to provide consulting services to our clients and to manage our business. The types of personal information we collect may include:

From Clients and Prospects

- Contact details (name, telephone number, email address, organisation name, position, office address)
- Business information (organisation size, industry, financial performance, operational metrics, strategic objectives)

- Engagement-related information (project scope, timelines, budgets, deliverables, communications)
- Meeting notes and correspondence
- Identification information (for client verification and engagement purposes)

From Employees, Contractors, and Service Providers

- Name, contact details, and identification information
- Employment or engagement history and qualifications
- Financial information (bank account details for payment purposes)
- Insurance and superannuation information (for employees)

Website Users

- IP address and device information
- Website usage data and analytics (including pages visited, time spent on site)
- Enquiry form submissions (name, email, message content)

Sensitive Information

We do not ordinarily collect sensitive information. However, if a consulting engagement requires collection of sensitive information (such as health information, racial or ethnic origin, or information about criminal records), we will only collect this with your explicit consent and for purposes directly related to the engagement.

4. How We Collect Personal Information

Direct Collection

We primarily collect personal information directly from you:

- Through face-to-face meetings and telephone conversations
- Via email correspondence
- Through our website contact forms and enquiry processes
- During engagement proposals and contracting processes
- Through project management and collaboration platforms
- In meetings, workshops, and presentations

Collection from Other Sources

In some circumstances, we collect personal information from other sources:

- From other organisations (with consent or where lawful and reasonable)
- From publicly available sources (business directories, organisation websites, professional networks)
- From third-party service providers who support our consulting delivery

- From clients or other stakeholders as part of engagement activities

Notification

When we collect personal information directly from you, we will take reasonable steps to notify you of the matters outlined in Section 5 (Purposes of Collection and Use). This notification will be provided at the time of collection or, where this is not practicable, as soon as possible afterward.

5. Purposes of Collection and Use

We collect, hold, and use personal information for the following purposes:

Primary Purposes

- Providing consulting services and delivering project deliverables
- Communicating with clients about engagements, timelines, and outcomes
- Understanding client organisations' context, challenges, and objectives
- Developing proposals and scopes of work
- Invoicing and managing payment for services
- Conducting project management and collaboration activities
- Providing ongoing support and follow-up after engagements

Business Development and Marketing

- Identifying and contacting prospective clients
- Maintaining a database of potential business opportunities
- Sending information about our services (only where we have consent or an existing relationship)
- Attending industry events and networking activities
- Responding to unsolicited enquiries

Business Management and Administration

- Managing our internal business operations
- Complying with legal and regulatory obligations
- Managing employee and contractor relationships
- Processing payments and managing financial records
- Protecting our legal interests and managing disputes

Website and Analytics

- Analysing website traffic and user behaviour
- Improving website functionality and user experience
- Tracking marketing campaign effectiveness

- Understanding client and prospect interests

Secondary Uses

We will not use personal information for a purpose other than the primary purpose without your consent, unless:

- The secondary use is directly related to the primary purpose, or
- We are required or authorised by law to use the information for the secondary purpose, or
- We have taken reasonable steps to provide you with notice of the secondary use and you have not objected.

6. How We Hold and Protect Personal Information

Information Held

Personal information is held in various formats, including:

- Electronic systems (project management software, email systems, client databases)
- Physical files (client files, engagement records, correspondence)
- Cloud-based storage services
- Backup systems and archives

Security Measures

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, and disclosure. Our security measures include:

- Access controls and user authentication (passwords, multi-factor authentication)
- Encryption of sensitive personal information in transit and at rest
- Physical security of office facilities and file storage areas
- Regular security updates and patches to systems
- Staff training and awareness on data protection and privacy obligations
- Limiting access to personal information to staff and contractors who have a legitimate business need
- Confidentiality obligations in employment and engagement agreements
- Regular review and testing of security measures

Limitations

While we implement reasonable security measures, no system is completely secure. We cannot guarantee absolute protection against unauthorised access, interference, loss, or disclosure. If you believe there has been a security incident affecting your personal information, please contact us immediately using the details in Section 12.

7. Data Retention and Disposal

We hold personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required by law.

Retention Periods

- Client engagement records: Generally retained for 7 years after project completion (or longer if required by law or relevant agreements)
- Prospect and business development information: Retained while relationship is active; updated or removed if contact is lost for 2+ years
- Website analytics data: Generally retained for 24 months
- Employee and contractor records: Retained for the duration of employment/engagement and typically 3-7 years afterward (as required by tax and employment law)
- Financial and tax records: Retained for 5 years in accordance with Australian Tax Office requirements

When personal information is no longer required, we securely destroy or de-identify it, unless we are required by law to retain it. Destruction methods include:

- Secure deletion of electronic data
- Shredding of physical documents
- Secure destruction of storage media

8. Disclosure of Personal Information

To Whom We Disclose

We may disclose personal information to the following categories of recipients for the purposes outlined above:

Third-Party Service Providers

We engage third-party service providers to support our business operations, including:

- Cloud storage and file management providers
- Project management and collaboration platform providers
- Email and communication service providers

- Accounting, bookkeeping, and tax advisory service providers
- Legal and professional advisors
- Website hosting and analytics providers
- Insurance providers
- Recruitment and staffing agencies

Professional Bodies and Regulators

We may disclose personal information to:

- Government agencies and regulators (where required or authorised by law)
- Professional standards bodies (if we are members or subject to regulation)
- Law enforcement and courts (if required by law or court order)

Related Entities

If Frank Partners is acquired, merged, or undergoes restructuring, personal information may be disclosed to related entities as part of that process.

Consent-Based Disclosures

We may disclose personal information to other parties where you have provided express consent.

Overseas Disclosure

We may disclose personal information to overseas recipients in limited circumstances:

- Where we engage overseas-based service providers (e.g., cloud service providers with servers overseas)
- Where clients or projects involve overseas stakeholders or delivery partners
- Where required by law

Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient protects your information in a substantially similar way to the Australian Privacy Principles, or we obtain your consent to the disclosure.

Key Overseas Disclosures

Common overseas recipients may include cloud service providers located in the United States, the European Union, or other countries. Specific countries will depend on your engagement and the service providers we use. If you require more detailed information about specific overseas disclosures, please contact us.

Contractors and Subcontractors

We require all third-party service providers and contractors to comply with privacy obligations equivalent to the Australian Privacy Principles. We include contractual obligations in all service agreements to protect personal information.

9. Your Privacy Rights and How to Exercise Them

Right to Access Personal Information

You have the right to access personal information about you that we hold. To request access, please provide your request in writing to our privacy contact (see Section 12). We will respond within a reasonable timeframe, typically 30 days.

We may charge a reasonable fee for providing access, which we will advise you of in advance. We may decline to provide access in certain circumstances permitted by law (for example, if providing access would be unlawful or would prejudice someone else's rights). If we decline to provide access, we will provide you with reasons.

Right to Seek Correction

If you believe personal information we hold about you is inaccurate, out-of-date, incomplete, irrelevant, or misleading, you have the right to request correction. To request correction, please contact us in writing with details of the correction you seek and the reasons for it.

We will take reasonable steps to correct the information. If we refuse to correct the information, we will provide you with written notice including:

- The reasons for the refusal
- How you can complain about the refusal
- Your right to request that we associate a statement with the information saying you believe it to be incorrect

Response timeframe for correction requests is typically 30 days.

Right to Request Deletion

While we may retain personal information for business, legal, or tax reasons, you may request that we delete personal information we hold about you. We will consider your request having regard to legal obligations and legitimate business interests. We will notify you of our decision.

10. Privacy Complaint Handling

How to Lodge a Complaint

If you believe Frank Partners has interfered with your privacy or breached the Australian Privacy Principles, you have the right to lodge a complaint. To lodge a complaint:

1. Contact us in writing using the contact details in Section 12, with details of:
    a. Your concern or complaint
    b. The specific privacy issue
    c. The outcome or remedy you are seeking
    d. Any supporting documentation
2. We will acknowledge your complaint within 10 business days and aim to investigate and respond within 30 days. If your complaint is complex, we will advise you of the expected timeframe.
3. We will investigate your complaint and provide a written response including:
    a. Our findings
    b. The actions we have taken or will take to address the complaint
    c. How you can escalate if you are not satisfied with our response

If you are not satisfied with our response to your privacy complaint, you may write to the Office of the Australian Information Commissioner (OAIC):

Website: www.oaic.gov.au
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Mail: GPO Box 3131, Canberra ACT 2601

The OAIC provides a free, independent, informal complaint process and can investigate privacy complaints about Australian organisations.

11. Website and Cookies

Website Privacy

When you visit our website, we collect certain information about your visit:

- Your IP address and browser type
- Pages visited and time spent on site
- Referring website and search terms
- Device information

This information is collected using website analytics tools (such as Google Analytics). While this information may not directly identify you, it may constitute personal information under the Privacy Act.

Third-Party Services

Our website may include links to third-party websites and services. We are not responsible for the privacy practices of these external sites. We encourage you to review their privacy statements before providing personal information.

12. Contact Information

For questions about this privacy statement, to exercise your privacy rights, or to lodge a privacy complaint, please contact:

Att: Privacy Officer
Phone: 0426668270
Address: Level 7, 80 Collins Street, Melbourne VIC 3000
Email: info@frankpartners.com.au

We will respond to all privacy enquiries and complaints within a reasonable timeframe and in accordance with the Australian Privacy Principles.

13. Changes to This Privacy Statement

Frank Partners may update this privacy statement from time to time to reflect changes to our privacy practices, legal requirements, or other matters. We will notify you of any material changes by:

- Publishing the updated statement on our website with an updated effective date
- Sending you written notice if you are an active client

Your continued use of our services or engagement with us following an update indicates your acceptance of the revised privacy statement.

14. Key Australian Privacy Principles Referenced in This Statement

This privacy statement is based on the following Australian Privacy Principles under the Privacy Act 1988 (Cth):

- APP 1: Open and transparent management of personal information
- APP 2: Anonymity and pseudonymity
- APP 3: Collection of solicited personal information
- APP 5: Notification about personal information management
- APP 6: Use or disclosure of personal information
- APP 8: Cross-border disclosure of personal information

- APP 10: Quality of personal information
- APP 11: Security of personal information
- APP 12: Access to personal information
- APP 13: Correction of personal information