BURSWOOD PARTNERS

PRIVACY, IDENTIFICATION AND VERIFICATION POLICY

1. Introduction

Burswood Partners Business Solutions Pty Ltd (Burswood Partners) is committed to protecting the privacy and confidentiality of personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

This Privacy Policy outlines how we collect, use, disclose, and manage personal information.

2. Purpose

This Privacy, Identification and Verification Policy explains how Burswood Partners collects, uses, stores, discloses and protects personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the firm's obligations under Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) legislation, the Tax Agent Service Act, Tax Agent Services (Code of Professional Conduct) and our professional and ethical standard obligations.

Burswood Partners is committed to protecting the privacy and confidentiality of personal and entity information while meeting its legal obligations to identify clients, verify identity information and conduct client due diligence (CDD) and enhanced client due diligence (ECDD) where required.

3. Types of Personal Information We Collect

Depending on the services provided, we may collect:

Identification Information

- Full name, date of birth, residential address, contact details
- Occupation, Tax File Number and Director ID Number (where authorised by acceptance of the Terms of Client Engagement),
- Driver's licence details, passport details, medicare card details and other accepted ID Documentation
- Entity information – Partnership, Company, Trust, Self-Managed Superannuation Fund information

AML/CTF Generated Information

For AML/CTF compliance purposes, we may collect information needed to:

- Verify and identify beneficial owners,
- Assess source of funds, and assess source of wealth where required
- Conduct sanctions screening
- Conduct politically exposed person (PEP) checks
- Perform client due diligence and if applicable, enhanced client due diligence

Business Information

- Financial and accounting records
- Taxation information
- Trust and corporate records and
- Engagement documents

4. How We Collect Personal and Entity Information

We collect personal and entity information directly from:

- Yourself
- From third parties, such as the Australian Taxation Office (ATO), ASIC, DFAT, Centrelink, Child Support Agency, any court, financial institutions, any other Government Department or Agencies, finance broker, financial planner, other business or your employer (with your consent)
- Depending on your entity structure we may collect from Directors, Trustees, Beneficial owners, and authorised representatives.
- When you complete our information collection forms, checklists or provide us with source documents.
- Third-party verification providers.
- Through our website (e.g. contact forms, cookies – see Section 15)

This Information may be obtained either;

- In person, phone, email or video conferencing
- Through our website
- Via secure client portals,
- Through identity verification software
- Through AML/CTF screening tools

5. Identity Verification Processes

Burswood Partners is required to verify the identity of all clients.

In addition, for clients where designated services are provided under our AUSTRAC AML / CTF obligations, we are required to complete additional processes such as Know Your Client (KYC) Client Due Diligence (CDD) and Enhanced Client Due Diligence (ECDD).

Collection

Burswood Partners may sight original identity documents, including but not limited to:

- Passport, Driver's licence, Birth certificate, Medicare card
- Company registration documents
- Trust documentation

Verification

Burswood Partners will:

- Examine the authenticity of documents
- Confirm the identity of the individual and / or entity
- Record that verification has occurred
- Document the date and method of verification

Document Retention

Where verification is completed, the firm will:

- Record that identity has been verified;
- Record the document type and verification details; and
- Not retain copies of personal identity documents unless required by law, necessary for compliance, requested by the client, or reasonably required to provide services.

This approach supports the principle of collecting and retaining only information that is reasonably necessary for Burswood Partners functions and activities.

6. Use of Third-Party Software Services for Identity Verification and AML Compliance

Burswood Partners may use third-party software services to assist with:

- AML/CTF processes such as Know Your Client (KYC) procedures, Client Due Diligence (CDD) and Enhanced Client Due Diligence (ECDD)
- Electronic Identity verification
- Beneficial ownership verification
- AML risk assessments and ongoing monitoring

When software is used, information entered into the system may be processed to verify identity and comply with AML/CTF requirements.

Burswood Partners use of software and is solely for legitimate business and regulatory compliance purposes.

7. Why We Collect and Use Personal Information

We collect and use personal information to:

- Provide accounting services
- Provide taxation services
- Provide designated services under the Anti-Money Laundering and Counter-Terrorism Financings Act 2006
- Establish and maintain client relationships
- Meet legal and regulatory obligations
- Verify identity
- Conduct KYC, CDD and ECDD processes
- Assess and manage AML/CTF risks

- Prevent fraud and financial crime
- Respond to legal requests and regulatory requirements
- Improve our services

8. Disclosure of Personal Information

We may disclose personal information to:

- Regulatory authorities
- AUSTRAC
- Australian Taxation Office
- Tax Practitioner Board
- Courts and tribunals
- Government agencies
- Professional advisers
- Technology providers
- Third-Party software identity verification providers
- External auditors
- Law enforcement agencies where legally required
- Requests for information under the Freedom of Information Act or Privacy Act (Federal or State Legislation).
- Institute of Public Accountants (IPA) if required in order to comply with our mandated Quality Review Program.

Information will only be disclosed where:

- Required by law; or
- Authorised by the individual; or
- Necessary for our legitimate business or compliance activities.

9. Overseas Disclosure

Some technology providers may store or process information outside Australia.

Where overseas disclosure occurs, we take reasonable steps to ensure service providers maintain privacy and security standards consistent with Australian privacy obligations.

10. Data Security

Burswood Partners implements reasonable security measures to protect personal information from:

- Misuse, interference, loss
- Unauthorised access, modification and disclosure

Controls may include:

- Multi-factor authentication, and encryption
- Secure document storage, access controls
- Staff confidentiality obligations
- Cybersecurity monitoring and
- Secure destruction processes

11. Retention and Destruction

We retain personal information only for as long as required to either:

- Provide services
- Meet legal and regulatory obligations
- Comply with AML/CTF record-keeping requirements
- Resolve disputes
- Protect legal rights

Information that is no longer required will be securely destroyed or de-identified.

Where manual identity verification has been performed and copies of identity documents have not been retained, records of the verification process may still be maintained for compliance purposes.

12. Access and Correction

Individuals may request access to personal information held by Burswood Partners and may also request correction of information that is:

- Inaccurate
- Incomplete
- Out of date
- Misleading

Requests should be made in writing to the Privacy Officer.

13. Privacy Complaints

Complaints regarding privacy matters may be directed to:

Privacy Officer
Burswood Partners
PO Box 600, South Perth WA 6951

PH: 08 9472 4944
Email: office.reception@burswoodpartners.com.au

Burswood Partners will investigate complaints and respond within a reasonable timeframe. If the complainant is not satisfied with the outcome, they may contact:

Office of the Australian Information Commissioner (OAIC)
Website: https://www.oaic.gov.au

14. AML/CTF Privacy Notice

Under Australia's AML/CTF laws, the Burswood Partners may be legally required to collect and verify personal information before providing certain services.

Failure to provide Burswood Partners with requested AML/CTF information may prevent the firm from commencing or continuing an engagement.

Burswood Partners may use collected information to:

- Verify identity
- Conduct KYC checks
- Conduct CDD and ECDD processes
- Assess AML/CTF risks
- Comply with reporting and record-keeping obligations

Burswood Partners cannot notify individuals when we are legally required to report certain matters to the governments financial intelligence agency (AUSTRAC). We will only report what the law strictly requires and will not disclose your information to authorities unless mandated by law.

15. Website Cookies

When a person visits our website, we may collect limited information via cookies and similar technologies. This helps us analyse website traffic and improve the user experience. Cookies can be managed in the settings via the utilised browser.

16. Applicable Legislation and APP/AML/CTF Alignment

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)
- AML/CTF Rules
- Tax Agent Services Act 2009 (where applicable)
- Tax Agent Services (Code of Professional Conduct) Determination 2024
- APES 110 Code of Ethics (where applicable)

This policy has been designed to align with:

- APP 1 – Open and Transparent Management of Personal Information
- APP 3 – Collection of Solicited Personal Information
- APP 5 – Notification of Collection
- APP 6 – Use and Disclosure
- APP 10 – Quality of Personal Information
- APP 11 – Security of Personal Information
- APP 12 – Access to Personal Information
- APP 13 – Correction of Personal Information

as well as AML/CTF requirements relating to client identification, client due diligence, enhanced client due diligence, ongoing monitoring and record keeping.