PRIVACY POLICY & DATA PROTECTION OBLIGATIONS

MELBOURNE BUILDING PRODUCTS PTY LTD

ABN: 67 661 544 040

DOCUMENT CONTROL & ADMINISTRATION

Document Reference	**Privacy, Data Protection & Consumer Guarantee Compliance Framework**
Effective Date	June 2026
Version	2.0 (Full Compliance Revision)
Approved By	Board of Directors, Melbourne Building Products Pty Ltd
Applicability	Public, Commercial Trade Portals, Builder Portals, In-Store Operations

---

1. STATUTORY FRAMEWORK, SCOPE & CORPORATE STATEMENT

1.1 Legislative Alignment & Jurisdiction

Melbourne Building Products Pty Ltd ("the Company", "we", "us", "our") is committed to protecting the privacy, confidentiality, and security of personal and commercial data in strict accordance with the Australian legal framework. This Privacy Policy outlines our institutional practices regarding the collection, holding, use, disclosure, and protection of personal information. It is drafted to satisfy our strict legal obligations under:

- The *Privacy Act 1988* (Cth) and the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
-

-

  The 13 Australian Privacy Principles (APPs) contained within Schedule 1 of the Privacy Act.
-
-

  The *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).
-
-

  The *Competition and Consumer Act 2010* (Cth), specifically Schedule 2 incorporating the **Australian Consumer Law (ACL)**.
-

1.2 Universal Scope of Application

This Policy governs all aspects of our business operations within the Commonwealth of Australia. This includes, but is not limited to, interactions at our physical brick-and-mortar storefronts, digital and e-commerce transactions, wholesale and trade account management, registered builder accounts, supply chain logistics, and post-sale consumer support.

1.3 Strategic Integration with the Australian Consumer Law (ACL)

As a specialist supplier of building products, components, and materials, the Company operates under stringent statutory obligations regarding product safety, consumer guarantees, returns, and warranties under the ACL. To validate claims, confirm structural liability, and ensure compliance with relevant building codes and product certifications, we must collect verifying credentials.

The collection of trade licences, building licences, compliance certificates, engineering specifications, and photographic installation evidence is a lawful, fair, and reasonable prerequisite to:

-

Assess and process statutory consumer guarantee claims and voluntary or extended manufacturer warranties.

-
- Authenticate that products were installed by a suitably qualified, licensed, and registered professional in accordance with manufacturer specifications and national building regulations.
-
- Mitigate corporate liability, prevent fraudulent warranty claims, and protect business assets from vexatious litigation or unjustified financial loss.
-

---

2. THE TYPES OF INFORMATION WE COLLECT

To effectively manage our corporate operations and fulfill our commercial and statutory duties, we collect and hold a range of personal and business information.

- **Identity & Contact Data:** Full legal name, corporate trading name, primary contact details, residential and business addresses, site/delivery addresses, email addresses, and phone numbers.
-
- **Commercial & Trade Verification Data:** Australian Business Numbers (ABNs), Australian Company Numbers (ACNs), building licences, trade certification numbers, and government-issued compliance forms.
-
- **Financial & Transaction Data:** Encrypted credit/debit card tokens, bank account details, credit applications, purchase histories, transaction ledgers, digital signatures, and credit history.

-
- **Security & Operational Surveillance:** Closed-circuit television (CCTV) video footage captured at our physical commercial premises, warehouse locations, and collection points.
-
- **Technical & Analytical Usage Data:** Internet Protocol (IP) addresses, device types, operating systems, browser configurations, and behavioral interaction metrics collected via cookies and tracking pixels.
-

2.1 Anonymity and Pseudonymity (APP 2)

Whenever it is lawful and practicable, you have the option of interacting with us anonymously or via a pseudonym (for example, general product pricing enquiries). However, under APP 2.2, we cannot provide this option where it is impracticable for us to deal with you, such as when creating trade accounts, processing secure credit card payments, delivering goods to a specific address, or verifying legal trade credentials for warranty processing.

---

3. METHODS & DIRECTNESS OF COLLECTION

3.1 Direct Collection Channels (APP 3)

In alignment with APP 3, we collect personal information only by lawful and fair means, and directly from you unless it is unreasonable or impracticable to do so. Direct collection occurs when you:

- Register for, apply to open, or maintain a Trade Account or Builder Account.
-
-

Execute a transaction online via our e-commerce infrastructure or in-store via Point-of-Sale (POS) systems.

Submit formal paperwork, including return forms, consumer guarantee requests, or warranty claims.

Engage with our customer service staff via email, telephonic communication, digital forms, or SMS text systems.

Enter physical operational areas of our business subject to active, signed CCTV surveillance.

3.2 Indirect Collection from Third Parties

Where it is necessary to collect information from a third party, we do so strictly within the confines of Australian law. This may include obtaining data from credit reporting bureaus (for trade credit applications), corporate registers (ASIC), or authorized representatives acting on your behalf (such as site foremen, project managers, or procurement officers).

---

4. PURPOSES OF COLLECTION, USE, AND DISCLOSURE

We operate under a strict "no sale" policy regarding personal data. We do not sell, rent, trade, or lease your personal information to third-party data brokers, competitors, or external retailers.

4.1 Primary Purposes (APP 6)

The Company collects, holds, uses, and discloses personal information for primary purposes directly tied to our business functions, including to:

- Establish, maintain, and verify credit limits and eligibility for trade and builder accounts.
- Process financial transactions, securely manage invoices, and facilitate logistics, freight, and site deliveries.
- Fulfill our consumer guarantee obligations under the ACL, including investigating product performance and verifying licensed installation.
- Detect, investigate, and prevent financial crimes, unauthorized account access, identity theft, and fraudulent merchant chargeback claims.
- Maintain workplace health and safety (WHS) standards and protect corporate property via physical surveillance.

4.2 Secondary Purposes and Direct Marketing (APP 7)

We will only use or disclose your personal information for a secondary purpose if you would reasonably expect us to do so, or where you have provided explicit consent.

Direct Marketing Compliance: We utilize personal data to provide tailored industry updates, trade pricing sheets, and promotional material only in compliance with the *Spam Act 2003* (Cth). Every electronic communication contains a prominent, clear, and functional "unsubscribe" mechanism. We will immediately cease all marketing communications upon receipt of an opt-out request.

4.3 Third-Party Operational Disclosures

To maintain efficient commercial operations, we may disclose specific, limited data elements to external service providers under strict confidentiality mandates:

- **Logistics Partners:** Freight forwarders, couriers, and third-party delivery networks.
- **Financial Infrastructure:** Secure, PCI-DSS compliant merchant gateways and credit assessment institutions.
- **Digital Optimization Platforms:** Hashed, pseudonymized data components may be communicated to secure advertising platforms (such as Google and Meta) strictly to optimize targeted business-to-business marketing campaigns.
- **Regulatory & Law Enforcement Authorities:** We reserve the right to disclose personal information to federal or state police, courts of competent jurisdiction, regulatory bodies (such as the OAIC or ACCC), or authorized insurance investigators where a statutory or legal obligation to disclose exists.

---

5. CROSS-BORDER DATA FLOWS & INTERNATIONAL TRANSFERS (APP 8)

The Company prioritizes local data sovereignty. All core corporate records, financial transactional histories, and trade account databases are securely hosted and maintained within servers located physically inside the Commonwealth of Australia.

However, some cloud-based enterprise software, data backup systems, or IT infrastructure utilities may utilize offshore storage nodes. Before disclosing any personal information to an overseas recipient, we take all reasonable steps required under APP 8.1 to ensure that the international recipient complies with the APPs or is subject to a legally binding data protection framework substantially similar to the *Privacy Act 1988* (Cth).

---

6. ACCOUNTS, SECURITY, AND COMMERCIAL LIABILITY SHIELD

6.1 Builder & Commercial Trade Accounts

The Company provides dedicated, password-protected online portals and commercial accounts (collectively, "Accounts") for verified builders, contractors, trade professionals, and corporate clients. These Accounts allow authorized users to access trade-tier pricing, view transaction histories, manage active projects, and execute commercial procurement orders.

6.2 Strict Responsibility for Access Credentials

The security, confidentiality, and integrity of all Account access credentials—including usernames, unique email identifiers, multi-factor authentication tokens, and passwords—remain **exclusively and entirely the responsibility of the registered Account holder (the "Account Holder", whether registered as a Builder or a Trade Client)**.

-

The Company takes no responsibility, and explicitly disclaims all liability, for any unauthorized access, data compromise, or security breaches resulting from an Account Holder's failure to maintain secure password protocols, share credentials among staff or third parties, or protect their local devices.

-
-

Account Holders are strictly required to implement robust password security measures and must immediately notify the Company in writing if they suspect their Account credentials have been compromised or exposed to unauthorized users.

-

6.3 Absolute Liability for Purchases & Financial Obligations

To the maximum extent permitted by Australian law, **the Account Holder assumes absolute financial and legal liability for any and all transactions, orders, purchases, or procurement contracts executed under their Account.**

-

Any purchase made using an Account Holder's unique login credentials, verified email link, or Account portal will be conclusively deemed authorized by the Account Holder.

-
-

In the event of unauthorized use, identity theft, or internal staff misuse of the Account, **the Account Holder remains wholly liable for the payment of all invoices, delivery fees, and associated debts incurred.**

-
-

The Company is under no legal obligation to verify the individual identity or specific corporate authorization of any person executing an order while logged into a valid, authenticated Builder or Trade Account.

-

---

7. INFORMATION SECURITY, STORAGE, & RETIONTION

7.1 Data Security Infrastructure (APP 11)

In strict compliance with APP 11, the Company implements rigorous administrative, physical, and technical safeguards designed to protect personal information from misuse, interference, loss, or unauthorized access, modification, and disclosure.

- **Encryption and Storage Controls:** Sensitive data assets—including corporate account files, trade registration documents, financial profiles, and contact registries—are held within access-controlled, firewalled environments using enterprise-grade encryption protocols.
-
- **Non-Encrypted Data Elements:** Standard operational logistics documents, including generalized historical order summaries, item specifications, and delivery dispatch notes, are held on secure internal operational systems to facilitate rapid customer lookup and warranty validation.
-

7.2 Technical Risk Acknowledgment

While the Company executes exhaustive, industry-standard cybersecurity measures to secure data holdings, no digital environment or internet transmission protocol can be certified as completely impervious to breach. The Company takes all reasonable steps mandated by Australian law to maintain data integrity, but notes that absolute security cannot be guaranteed against sophisticated, unlawful cyber-warfare or malicious state-actor intrusions.

7.3 Data Destruction and De-identification

We retain personal information only for as long as necessary to fulfill the primary purposes for which it was collected, or to satisfy statutory record-keeping mandates under Australian tax and corporations law (typically 7 years). Once information is no longer required, we take immediate, irreversible steps to securely destroy electronic records or permanently de-identify the data.

---

8. NOTIFIABLE DATA BREACHES (NDB) SCHEME COMPLIANCE

In accordance with Part IIIC of the *Privacy Act 1988* (Cth), the Company maintains an active Data Breach Response Plan. In the event of an unauthorized access, disclosure, or loss of personal information that is deemed likely to result in serious harm to any affected individual:

1.

Immediate Containment: We will immediately implement technical and physical controls to contain the breach and minimize data exposure.

2.

3.

Expeditious Assessment: We will conduct a thorough, expedited assessment of the incident within the legally mandated 30-day window.

4.

5.

Statutory Notification: If an eligible data breach is verified, we will issue a formal statement to the Office of the Australian Information Commissioner (OAIC) and directly notify all affected individuals as soon as practicable. This notification will include a comprehensive description of the breach, the specific categories of data exposed, and actionable steps individuals should take to mitigate potential adverse impacts.

6.

---

9. DATA QUALITY, ACCESS, AND RECTIFICATION RIGHTS

9.1 Accuracy of Personal Holdings (APP 10)

We take all reasonable steps to ensure that the personal information we collect, use, and disclose is accurate, up-to-date, complete, and relevant to our operational activities.

9.2 Right of Access (APP 12)

Under APP 12, you possess a statutory right to request access to the personal information held about you by the Company. All requests must be submitted in writing to our Privacy Officer. We will respond within a reasonable timeframe (typically 30 business days).

- **Statutory Exceptions:** We reserve the right to refuse access in limited circumstances permitted under APP 12.3, such as where providing access would pose a serious threat to the life or health of any individual, unreasonably impact the privacy of others, or prejudice ongoing legal proceedings or negotiations.
-

9.3 Right of Correction (APP 13)

If you establish that the personal information we hold about you is inaccurate, out of date, incomplete, irrelevant, or misleading, you may submit a formal request for rectification. Upon verification, we will take immediate, reasonable steps to amend our records at no cost to you.

---

10. INQUIRIES, COMPLAINTS, AND CORPORATE CONTACT DETAILS

If you have any questions concerning this Privacy Policy, wish to exercise your data access rights, or believe that the Company has breached its obligations under the APPs or the Privacy Act, you may lodge a formal complaint with our compliance team.

Privacy Compliance Officer

Melbourne Building Products Pty Ltd

Postal Address: 1/11 Dazln Drive, Melton VIC 3338

Email Interface: info@melbournebuildingproducts.com.au

Telephone Contact: 0449281788

10.1 External Escalation Mechanisms

We treat all privacy complaints with high priority and will investigate and respond to your concerns in writing within 30 days. If you remain dissatisfied with our internal resolution framework, you maintain the statutory right to escalate your complaint directly to the external regulatory authority:

The Office of the Australian Information Commissioner (OAIC)

GPO Box 5218, Sydney NSW 2001

Web Interface: www.oaic.gov.au

Telephone: 1300 363 992