AUSTRALIAN BUILDING COMPANY PRIVACY POLICY

Effective date:
Last reviewed:
Next scheduled review:
Version: 1.0

1. INTRODUCTION AND OVERVIEW

1.1 Who We Are

1.1.1 Australian Building Company is a major Australian residential home builder operating across Australia (including through offices, display homes, design studios, and construction sites) and providing services throughout the residential home building journey, including initial enquiry, design and selections, contracting, construction, handover, and warranty support.

1.1.2 In this Privacy Policy, **Australian Building Company**, **we**, **us** and **our** refers to the Australian Building Company group of entities that collect, hold, use and disclose personal information in connection with Australian Building Company's operations in Australia (including related bodies corporate and business units that support our residential construction activities). Entities include: Metricon Homes Pty Ltd, Metricon Homes Queensland Pty Ltd, Australian Building Company Pty Ltd, Australian Building Company Queensland Pty Ltd and Newfield Real Estate Pty Ltd, Gemaro 005 Pty Ltd.

1.1.3 We are committed to protecting the privacy of individuals whose personal information we handle, and to managing personal information in an open and transparent way.

1.2 Purpose of This Privacy Policy

1.2.1 This Privacy Policy explains how we collect, hold, use and disclose personal information, and how you may access and correct personal information we hold about you or make a privacy complaint.

1.2.2 This Privacy Policy is intended to support compliance with the *Privacy Act 1988 (Cth)* (Privacy Act), including the **Australian Privacy Principles** (APPs), and the **Notifiable Data Breaches** (NDB) scheme.

1.2.3 This Privacy Policy is designed for the residential construction sector and addresses common data touchpoints in the home building journey, including:

- initial enquiries and display home visits;
- design consultations and selections appointments;
- tendering, contracting, variations and progress claims;
- construction site access and safety controls;
- handover and customer care; and
- warranty and defect management.

1.3 Scope and Application

1.3.1 This Privacy Policy applies to personal information we collect and handle about:

- prospective customers (including people who enquire, attend a display home, request a quote, request a tender, or use our online tools);
- customers and contract holders (including owners, co-owners, guarantors, and authorised representatives);
- visitors to our display homes, offices, design studios and construction sites (including for safety and security purposes);
- suppliers, subcontractors, consultants and other business partners (including their personnel);
- job applicants and individuals who work for or with us (including employees and contractors), to the extent the Privacy Act applies; and
- users of our websites, digital services, and social media channels.

1.3.2 This Privacy Policy applies to personal information collected in Australia and, where relevant, personal information disclosed to or handled by overseas recipients as described in **Section 7 (Overseas disclosures and cross-border transfers)**.

1.3.3 This Privacy Policy does not apply to:

- information that is not "personal information" under the Privacy Act (for example, information that has been irreversibly anonymised); or
- third-party websites, platforms or services that we do not control (even if linked from our websites). Those third parties are responsible for their own privacy practices.

1.4 Legal Framework and Compliance

1.4.1 We manage personal information in accordance with:

- the *Privacy Act 1988 (Cth)* and the APPs (including APP 1 (open and transparent management of personal information), APP 3 (collection), APP 5 (notification), APP 6 (use and disclosure), APP 7 (direct marketing), APP 8 (cross-border disclosure), APP 10 (quality), APP 11 (security), APP 12 (access) and APP 13 (correction)); and
- the NDB scheme in Part IIIC of the Privacy Act (including assessment and notification obligations for eligible data breaches).

1.4.2 We also recognise that our operations interact with a range of legal and regulatory requirements relevant to residential construction and associated activities (including contracting, safety, and warranty support). Where those requirements require us to collect, use, retain or disclose information, we do so in a manner intended to be consistent with the Privacy Act.

1.4.3 Where we handle personal information in connection with finance facilitation through partners (for example, where you request introductions to mortgage brokers or lenders), additional terms and privacy notices of those partners may apply to their handling of your information.

1.5 Definitions and Key Terms

In this Privacy Policy:

1.5.1 **AI** means artificial intelligence technologies, including machine learning models and automated tools that may process data to generate predictions, recommendations, classifications, summaries or responses.

1.5.2 **APPs** means the Australian Privacy Principles in Schedule 1 to the Privacy Act.

1.5.3 **authorised representative** means a person you authorise to act on your behalf (for example, a spouse/partner, family member, lawyer, conveyancer, broker, or agent).

1.5.4 **biometric information** has the meaning given in the Privacy Act and is a type of sensitive information.

1.5.5 **building contract** means a contract for residential building works (including associated documents such as specifications, plans, selections, variations, and progress claim documentation).

1.5.6 **collection** includes gathering, acquiring or obtaining personal information by any means.

1.5.7 **complaint** means a complaint about how we have handled personal information.

1.5.8 **construction site** includes any site at which we or our contractors perform residential building works, including display home construction sites.

1.5.9 **credit-related information** has the meaning given in the Privacy Act (including credit information and credit eligibility information), where applicable.

1.5.10 **customer** means an individual who acquires or seeks to acquire our residential building services or related services.

1.5.11 **data breach** means unauthorised access to, unauthorised disclosure of, or loss of, personal information.

1.5.12 **direct marketing** has the meaning in the Privacy Act and includes marketing communications sent directly to an individual.

1.5.13 **disclosure** means making personal information available or accessible to others outside our effective control and management.

1.5.14 **eligible data breach** has the meaning given in the Privacy Act (including where a data breach is likely to result in serious harm and we have not been able to prevent that likelihood through remedial action).

1.5.15 **financial information** includes information relating to your financial position, income, expenses, assets, liabilities, banking details, payment history, and finance application details.

1.5.16 **government identifier** has the meaning given in the Privacy Act (for example, driver licence number, passport number, Medicare number).

1.5.17 **hold** includes possessing or controlling a record that contains personal information.

1.5.18 **identity verification** means steps taken to confirm an individual's identity (including to prevent fraud and unauthorised access).

1.5.19 **marketing partners** means third parties who assist us with marketing, advertising, analytics, campaign delivery, or audience targeting.

1.5.20 **NDB scheme** means the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

1.5.21 **OAIC** means the Office of the Australian Information Commissioner.

1.5.22 **personal information** has the meaning in the Privacy Act: information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.

1.5.23 **Privacy Act** means the *Privacy Act 1988 (Cth)*.

1.5.24 **Privacy Officer** means the person or team appointed by Australian Building Company to manage privacy enquiries and complaints (see **Section 20**).

1.5.25 **related bodies corporate** has the meaning given in the *Corporations Act 2001 (Cth)*.

1.5.26 **residential construction sector** means the industry and activities associated with designing, contracting, building and warranting residential homes, including associated supply chains and services.

1.5.27 **safety registration** includes visitor sign-in records, inductions, access permissions, incident reports, and emergency contact details used to manage safety and security.

1.5.28 **sensitive information** has the meaning in the Privacy Act and includes health information and other information listed as sensitive information.

1.5.29 **service providers** means third parties who provide services to us (including IT, cloud hosting, customer support, analytics, security, professional services, and administrative support).

1.5.30 **use** means handling personal information within our organisation, including accessing and analysing it.

1.5.31 **warranty period** means the period during which we provide warranty support and defect management services (including any statutory or contractual warranty periods applicable to residential building works).

2. TYPES OF PERSONAL INFORMATION WE COLLECT

2.1 Customer Information - Prospective Buyers

2.1.1 We may collect personal information from prospective customers at the early stages of the home building journey, including when you:

- enquire online, by phone, or in person;
- attend a display home, design studio, or sales office;
- request a brochure, price estimate, tender, or quote;
- participate in an appointment, consultation, or event; or
- use our online tools.

2.1.2 The personal information we may collect includes:

- identification and contact details (for example, name, address, email, phone number);
- preferred contact method and communication preferences;
- property and project details (for example, suburb, land status, lot details, site constraints, anticipated build timeframe);
- home preferences and lifestyle requirements (for example, preferred designs, floorplan preferences, number of bedrooms, accessibility preferences);
- household and family composition information (for example, number of occupants, multigenerational living requirements), where relevant to design and suitability discussions;
- budget range and high-level financial capacity information (for example, indicative borrowing capacity, deposit readiness), where you choose to provide it; and
- information you provide in communications with us (including meeting notes and enquiry history).

2.1.3 Where you attend a display home or office, we may also collect information for safety, security and operational purposes, including sign-in details and CCTV footage (see **Section 3.4**).

2.2 Customer Information - Contract Holders

2.2.1 If you proceed to tendering, contracting, construction and warranty support, we may collect more detailed personal information necessary to deliver residential building services and manage our contractual relationship with you.

2.2.2 This may include:

- identity information (including copies of identity documents where required for verification or fraud prevention);
- date of birth (where required for identification, finance facilitation, or verification processes);
- detailed contact information for owners, co-owners, and authorised representatives;
- billing and payment contact details;
- information about your land (including title details or land settlement timing where relevant to project planning);
- building contract documents and related records (including plans, specifications, selections, variations, and correspondence);
- information relevant to construction delivery (including access arrangements, special site conditions, and scheduling constraints);
- customer care and warranty records (including defect reports, inspection notes, rectification scheduling, and communications);
- information about your authorised representatives and third parties involved in your project (for example, brokers, conveyancers, lawyers), where you provide those details or authorise contact; and
- records of consents, preferences and requests you make (including marketing preferences and privacy-related requests).

2.3 Sensitive Information Collection

2.3.1 We generally do not seek to collect sensitive information unless it is reasonably necessary for our functions or activities and we are permitted to do so under the Privacy Act.

2.3.2 In the residential construction context, sensitive information may be collected where you choose to provide it or where it is necessary to support your requirements, for example:

- **health information** relevant to accessibility or mobility requirements (for example, to support design choices such as step-free access or bathroom modifications);
- information indicating a need for additional support or accommodations when attending sites or appointments; and
- information that may be sensitive because it relates to personal circumstances you disclose (for example, hardship-related circumstances), where relevant to managing your account, communications and arrangements.

2.3.3 Where we collect sensitive information, we take additional care in handling and securing it (see **Section 8**).

2.4 Financial and Banking Information

2.4.1 We may collect financial and banking information where reasonably necessary to:

- manage deposits and progress payments;
- assess and manage payment risk;
- support finance facilitation through partners (where you request it);
- manage refunds, credits, adjustments or reconciliations; and

- manage debt recovery (where applicable).

2.4.2 This may include:

- bank account details (account name, BSB, account number);
- payment transaction details (including receipts and remittance information);
- finance-related documents you provide (for example, pre-approval letters or loan documentation), where relevant to scheduling and contract management; and
- information about your financial position where you provide it for the purposes of progressing your project.

2.4.3 We do not use banking information to create direct marketing lists.

2.5 Site and Safety Information

2.5.1 We may collect personal information to manage safety and security at our offices, display homes and construction sites, including:

- visitor registrations and sign-in/sign-out records;
- site induction records and acknowledgements;
- access permissions and access logs (where access control systems are used);
- emergency contact details (where required for site access or inductions);
- incident, hazard and near-miss reports (including witness details where relevant); and
- contractor and subcontractor personnel details required for site access and compliance management.

2.5.2 We may require individuals to comply with site rules and safety processes as a condition of entry to construction sites, including maintaining accurate visitor and induction records.

2.6 Digital and Online Information

2.6.1 When you interact with our websites, digital tools or online services, we may collect:

- device and browser information;
- IP address and approximate location information derived from IP address;
- website usage information (pages viewed, time spent, referring pages);
- form submission data (including enquiry forms and appointment requests);
- preferences saved in digital tools (for example, saved designs or selections, where functionality exists); and
- cookie and tracking data as described in **Section 12.5**.

2.6.2 We may also collect information from social media interactions where you engage with our official pages or content, subject to the settings and policies of the relevant platform.

2.7 Communication Records

2.7.1 We may keep records of communications with you across channels, including:

- emails and email attachments;
- phone call records and, where used, call recordings (with appropriate notice);
- SMS and messaging communications;
- video conference records (including meeting notes and action items); and
- in-person meeting notes (including design consultation notes and selections outcomes).

2.7.2 These records support contract administration, customer service, quality assurance, dispute handling, and warranty support.

2.8 Third-Party Information

2.8.1 We may collect personal information about you from third parties where it is reasonably necessary for our functions and activities, including:

- authorised representatives (for example, where a family member or agent communicates on your behalf);
- mortgage brokers, lenders and finance partners (where you request finance facilitation);
- suppliers and subcontractors (for example, where they report site access issues, delivery coordination details, or warranty-related information);
- professional advisers (for example, lawyers or conveyancers where you authorise them to liaise with us); and
- publicly available sources where appropriate (for example, to confirm business contact details of suppliers).

2.8.2 If you provide us with personal information about another person (for example, a co-owner, guarantor, emergency contact, or authorised representative), you must ensure you have authority to do so and that the person is aware of this Privacy Policy where appropriate.

3. HOW WE COLLECT PERSONAL INFORMATION

3.1 Direct Collection Methods

3.1.1 We collect personal information directly from you when you:

- complete forms (online or paper), including enquiry, appointment, tender or contract documentation;
- speak with our staff at display homes, offices, design studios or on site;
- communicate with us by phone, email, SMS or other channels;
- participate in surveys, feedback processes, promotions or events;
- make payments or provide banking details for refunds or payments; and
- submit warranty requests, defect reports, or customer care enquiries.

3.1.2 We aim to collect only the personal information that is reasonably necessary for our functions and activities.

3.1.3 Where practical, we will give you the option to interact with us anonymously or using a pseudonym, but this may not be possible for most residential building services (for example, where we need to prepare a tender, enter into a building contract, manage payments, or coordinate construction and warranty services).

3.2 Indirect Collection Sources

3.2.1 We may collect personal information indirectly where:

- you authorise a third party to provide information to us (for example, your broker, lawyer, conveyancer or agent);
- it is unreasonable or impracticable to collect the information directly from you; or
- we are otherwise permitted to do so under the Privacy Act.

3.2.2 Where required by APP 5, we will take reasonable steps to notify you of the collection and the matters required to be notified, including the purposes of collection and how you may access this Privacy Policy.

3.3 Technology-Based Collection

3.3.1 We may collect personal information automatically through technology when you use our websites and digital services, including through:

- cookies and similar technologies;
- analytics tools;
- customer relationship management (CRM) systems;
- integrated scheduling, customer service and business platforms; and
- security monitoring tools used to protect our systems.

3.3.2 For further detail, see **Section 12 (Website, mobile apps, and digital services)**.

3.4 Surveillance and Recording

3.4.1 We may use CCTV and other security systems at some locations (including offices and display homes) for safety, security, incident investigation and loss prevention.

3.4.2 We may take photographs or videos on construction sites for legitimate business purposes, including progress tracking, quality assurance, defect identification, and warranty rectification planning. Where those images include individuals, they may constitute personal information.

3.4.3 We may record calls or maintain call logs for training, quality assurance, and dispute resolution purposes, where permitted by law and with appropriate notice.

3.5 Collection from Minors

3.5.1 Our products and services are generally directed to adults. However, we may collect limited information relating to minors where:

- it is provided by a parent/guardian for design and household planning purposes; or
- it is necessary for safety and security (for example, visitor management at a display home).

3.5.2 We take reasonable steps to avoid collecting unnecessary personal information about minors and to handle any such information with appropriate care and security.

4. PURPOSES FOR COLLECTION AND USE

4.1 Primary Business Functions

4.1.1 We collect, hold and use personal information to conduct our residential construction business, including to:

- respond to enquiries and provide information about home designs, inclusions, pricing and availability;
- arrange and manage appointments (including display home visits and design consultations);
- prepare estimates, quotes, tenders and proposals;
- enter into, administer and perform building contracts (including variations);
- coordinate construction delivery, including scheduling, site supervision and trade coordination;
- manage selections, upgrades and customer preferences;
- provide customer updates and manage communications throughout the build;
- manage handover processes and post-handover support; and
- provide warranty and defect management services during the warranty period.

4.1.2 We may also use personal information to manage and improve our internal processes, including workforce planning, operational reporting, and service improvement.

4.2 Legal and Regulatory Compliance

4.2.1 We may use and disclose personal information as reasonably necessary to comply with applicable laws and regulatory requirements, including:

- responding to lawful requests and directions from regulators and authorities;
- maintaining records required for compliance and audit purposes;
- managing safety and security obligations at our workplaces and construction sites; and
- managing complaints, disputes, and legal claims.

4.2.2 Where we are required by law to collect particular information, we will generally inform you of that requirement at or around the time of collection.

4.3 Customer Service and Communication

4.3.1 We use personal information to support customer service, including to:

- provide progress updates and respond to questions;
- manage change requests and variations;
- coordinate site meetings and inspections;
- manage customer care and warranty requests; and
- handle complaints and disputes.

4.3.2 We may use communication records to maintain continuity of service, reduce repetition, and improve accuracy in responding to customer needs.

4.4 Marketing and Business Development

4.4.1 We may use personal information to:

- send you information about our designs, promotions, events, and services;
- invite you to provide feedback or participate in surveys;
- conduct market research and improve our offerings; and
- develop and measure the effectiveness of marketing campaigns.

4.4.2 We manage direct marketing in accordance with APP 7 and applicable marketing laws (see **Section 11**).

4.5 Financial Management and Credit Assessment

4.5.1 We use personal information for financial administration and risk management, including to:

- process deposits and progress payments;
- issue invoices and receipts;
- manage refunds and adjustments;
- manage payment arrangements; and
- manage overdue accounts and debt recovery processes (where applicable).

4.5.2 Where you request finance facilitation through partners, we may use and disclose information to support that process as described in **Section 6.3**.

4.6 Quality Improvement and Analytics

4.6.1 We may use personal information (including aggregated insights derived from personal information) to:

- measure customer satisfaction and service performance;
- identify trends in design preferences and product performance;
- improve construction processes, scheduling and quality outcomes;
- improve warranty response times and defect prevention; and
- develop training and operational improvements.

4.6.2 Where practicable, we use de-identified or aggregated data for analytics and reporting.

4.7 Safety and Security

4.7.1 We use personal information to maintain safety and security, including to:

- manage visitor registrations and site access controls;
- administer site inductions and safety compliance;
- investigate incidents, hazards and near misses;
- respond to emergencies; and
- prevent, detect and respond to security threats and fraud.

5. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

5.1 AI Systems Overview

5.1.1 We may use AI-enabled tools within parts of our business to support efficiency, service quality, and operational improvement in the residential construction context.

5.1.2 AI may be used in systems and workflows such as:

- customer service enhancements (for example, assisting with responding to common enquiries and routing requests to appropriate teams);
- data analytics and reporting (for example, identifying trends in enquiry volumes, build stages, or warranty categories);
- business process efficiency (for example, summarising internal notes, assisting staff to locate relevant information, or improving internal workflows); and
- operational planning (for example, supporting scheduling and resource planning through data-driven insights).

5.1.3 We design and use AI tools to support, not replace, appropriate human judgement in customer-facing and contract-critical decisions.

5.2 Automated Decision-Making Processes

5.2.1 Some systems we use may involve automated processing that generates outputs such as recommendations, prioritisation, categorisation or risk flags.

5.2.2 In the home building journey, automated processing may be used to assist with:

- triaging and routing enquiries to the right team;
- identifying the likely category of a customer care or warranty request based on information provided;
- generating draft responses or summaries for staff review; and
- producing operational forecasts (for example, anticipated volumes of customer service requests).

5.2.3 Where an automated process materially affects you (for example, if it determines priority handling of a request or influences an outcome), we take steps to ensure there is appropriate oversight.

5.3 Data Analytics and Machine Learning

5.3.1 We may use personal information (and/or de-identified information derived from it) to:

- improve customer experience across enquiry, design, build and warranty stages;
- identify common issues and improve quality outcomes;
- improve operational efficiency (including scheduling and resource allocation); and
- measure and improve marketing effectiveness.

5.3.2 Where practicable, we limit the use of identifiable personal information in analytics and prefer aggregated or de-identified datasets.

5.4 Transparency and Human Oversight

5.4.1 We aim to be transparent about our use of AI and automated processing. Where required by the Privacy Act (including APP 1 and APP 5), we will provide notice of collection and relevant handling practices.

5.4.2 You may:

- request information about how we handle your personal information, including whether we use automated processing in connection with your interactions.

5.4.3 We may not be able to provide full details of AI system logic where doing so would compromise security, reveal confidential commercial information, or be otherwise restricted by law; however, we will provide meaningful information where reasonably possible, including the types of data used and the nature of the output.

5.5 AI Data Security and Accuracy

5.5.1 We apply security controls to AI-enabled systems consistent with our broader information security program (see **Section 8**), including access controls, monitoring, and vendor management.

5.5.2 We take reasonable steps to ensure personal information used in AI-enabled processes is accurate, up-to-date and complete for the purpose for which it is used (APP 10).

5.5.3 We take reasonable steps to mitigate risks associated with AI outputs, including:

- human review of AI-generated content where used for customer communications or contract administration;
- quality assurance checks and monitoring for errors; and

- controls to reduce inappropriate bias or unfair outcomes where AI is used for categorisation or prioritisation.

6. DISCLOSURE OF PERSONAL INFORMATION

6.1 Internal Disclosures

6.1.1 We may disclose personal information within the Australian Building Company group (including related bodies corporate and business units) where reasonably necessary to:

- respond to enquiries and provide services;
- administer building contracts and deliver construction services;
- provide customer care and warranty support;
- manage safety and security; and
- support shared corporate functions (for example, IT, finance, legal, risk, audit, and compliance).

6.1.2 We take reasonable steps to ensure internal access is limited to personnel who need the information for their role (see **Section 14.3**).

6.2 Construction Industry Partners

6.2.1 We may disclose personal information to subcontractors, suppliers and trade contractors where reasonably necessary to:

- deliver construction services;
- coordinate site access, scheduling and deliveries;
- manage defects, rectification works and warranty claims; and
- obtain manufacturer warranties and service support for installed products and appliances.

6.2.2 Disclosures may include contact details, site address, relevant scheduling information, and information about the works required.

6.2.3 We take reasonable steps to limit disclosures to what is necessary for the relevant purpose.

6.3 Financial Services Partners

6.3.1 Where you request finance facilitation, we may disclose personal information to third parties such as:

- mortgage brokers;
- lenders and finance providers;
- valuers; and
- insurers (where relevant to the finance process).

6.3.2 The information disclosed may include contact details and information relevant to your finance enquiry or application, as authorised by you or as reasonably necessary to facilitate the requested service.

6.3.3 Those third parties will handle your personal information under their own privacy policies and legal obligations.

6.4 Government and Regulatory Bodies

6.4.1 We may disclose personal information to government agencies, regulators and other authorities where required or authorised by law, including in connection with:

- building and planning processes;
- safety and incident reporting;
- compliance audits and investigations; and
- responding to lawful requests (including subpoenas, notices and court/tribunal orders).

6.5 Professional Service Providers

6.5.1 We may disclose personal information to professional advisers and service providers who assist our business, including:

- lawyers and legal service providers;
- accountants and auditors;
- consultants;
- IT and cybersecurity providers;
- marketing agencies and analytics providers; and
- customer support platform providers.

6.5.2 We take reasonable steps to require service providers to handle personal information consistently with our instructions and to implement appropriate security measures.

6.6 Emergency and Legal Disclosures

6.6.1 We may disclose personal information where we reasonably believe it is necessary to:

- lessen or prevent a serious threat to life, health or safety;
- respond to an emergency or incident at a construction site or premises;
- investigate suspected unlawful activity, fraud, or security incidents; or
- establish, exercise or defend legal rights.

7. OVERSEAS DISCLOSURES AND CROSS-BORDER TRANSFERS

7.1 Overseas Recipients Overview

7.1.1 We may disclose personal information to overseas recipients, or store or process personal information in systems located overseas, where reasonably necessary for our operations.

7.1.2 Overseas jurisdictions may include, but are not limited to:

- **the Philippines, China and Vietnam** (for example, administrative processing and support services such as drafting and estimating);
- **New Zealand** (for example, regional support services); and
- **the United States** (for example, cloud storage, software platforms, and IT support).

7.1.3 We may also use service providers with global operations, which may involve storage or processing in multiple jurisdictions.

7.2 Cloud Storage and IT Services

7.2.1 We may use cloud-based software and infrastructure to store and process personal information, including customer relationship management, document management, email, collaboration tools, and customer support systems.

7.2.2 Where cloud service providers host or process data overseas, this may involve cross-border disclosure under APP 8.

7.2.3 We take reasonable steps to select reputable providers and implement contractual and technical safeguards as described in **Section 7.4** and **Section 8**.

7.3 International Service Providers

7.3.1 We may disclose personal information to international service providers who assist with:

- IT support and maintenance;
- cloud hosting and data storage;
- customer service and administrative processing; and
- software development, monitoring and security operations.

7.3.2 Disclosures are limited to what is reasonably necessary for the service being provided.

7.4 Cross-Border Transfer Safeguards

7.4.1 Where APP 8 applies, we take reasonable steps to ensure overseas recipients handle personal information in a manner consistent with the APPs. Depending on the circumstances, safeguards may include:

- contractual obligations requiring appropriate privacy and security controls;
- restrictions on use and disclosure;
- confidentiality obligations;
- audit and assurance rights (where appropriate);

- incident notification obligations; and
- security requirements aligned to the sensitivity of the information.

7.4.2 We remain accountable for cross-border disclosures where required by the Privacy Act.

7.5 Customer Rights and Cross-Border Transfers

7.5.1 You may contact us to request further information about our overseas disclosures and the categories of overseas recipients we use (see **Section 20**).

7.5.2 If you have concerns about overseas handling of your personal information, you may make a complaint in accordance with **Section 10.4** and **Section 18**.

8. DATA SECURITY AND PROTECTION MEASURES

8.1 Technical Security Controls

8.1.1 We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11).

8.1.2 Our technical controls may include:

- role-based access controls and authentication measures;
- logging and monitoring of system access;
- network security controls (including firewalls and threat detection);
- encryption in transit and, where appropriate, encryption at rest;
- secure configuration and patch management;
- malware protection and endpoint security controls;
- secure backups and recovery processes; and
- segregation of environments and least-privilege access principles.

8.1.3 We apply additional controls where we handle higher-risk data (for example, financial information and identity documents).

8.2 Physical Security Measures

8.2.1 We use physical security measures to protect hard copy records and on-site systems, which may include:

- controlled access to offices and secure areas;
- visitor management processes;
- secure storage for paper records (including locked cabinets and restricted-access rooms);
- secure printing practices where appropriate; and
- secure disposal and destruction of documents.

8.3 Administrative and Procedural Safeguards

8.3.1 We maintain governance and procedures to support privacy and security, which may include:

- privacy and security policies and internal standards;
- staff training and awareness programs (see **Section 14.1**);
- incident response procedures (see **Section 16**);
- access reviews and user lifecycle management;
- privacy impact assessments for relevant initiatives (see **Section 15.2**); and
- vendor and third-party risk management (see **Section 8.4**).

8.4 Third-Party Security Requirements

8.4.1 Where service providers handle personal information on our behalf, we take reasonable steps to ensure they implement appropriate security measures, which may include:

- contractual privacy and confidentiality obligations;
- security questionnaires and due diligence;
- restrictions on subcontracting and offshore processing where appropriate;
- breach notification requirements; and
- ongoing monitoring and review proportionate to risk.

8.5 Data Breach Prevention and Response

8.5.1 We maintain processes designed to prevent, detect and respond to data breaches, including:

- monitoring and alerting processes;
- investigation and containment procedures;
- assessment of whether a breach is an eligible data breach under the Privacy Act; and
- notification processes to affected individuals and the OAIC where required.

8.5.2 Further detail is set out in **Section 16 (Notifiable data breaches and incident response)**.

9. DATA RETENTION AND DESTRUCTION

9.1 Retention Principles and Legal Requirements

9.1.1 We retain personal information only for as long as necessary to fulfil the purposes for which it was collected, or for related purposes permitted by the Privacy Act, unless a longer retention period is required or authorised by law.

9.1.2 Retention periods may be influenced by:

- contractual obligations (including building contract administration);
- warranty and defect management requirements across the warranty period;
- dispute resolution and complaint handling needs; and

- legal and regulatory requirements (including record-keeping obligations).

9.2 Customer Lifecycle Retention Periods

9.2.1 We may retain different categories of personal information for different periods depending on the stage of the customer journey, including:

- **initial enquiry stage**: enquiry records and communications to manage follow-up and service quality;
- **tender and contracting stage**: documents and communications necessary to form and administer the building contract;
- **construction stage**: scheduling, site, quality assurance and communications records;
- **handover stage**: handover documentation and customer care records; and
- **warranty stage**: warranty requests, defect reports, inspection records and rectification documentation.

9.2.2 Where a customer does not proceed beyond an early stage, we may retain enquiry records for a period consistent with business needs, compliance requirements and dispute management, and then securely destroy or de-identify them.

9.3 Legal and Regulatory Retention Obligations

9.3.1 We may retain certain records to comply with legal and regulatory obligations, including where retention is necessary for:

- responding to regulators and authorities;
- managing legal claims and disputes; and
- audit and compliance activities.

9.4 Secure Destruction Procedures

9.4.1 When personal information is no longer required, we take reasonable steps to destroy or de-identify it in a secure manner.

9.4.2 Destruction methods may include:

- secure shredding of paper records; and
- secure deletion or sanitisation of electronic records, including from backups where reasonably practicable in accordance with system constraints and retention cycles.

9.5 Archive and Long-Term Storage

9.5.1 We may archive certain information for legitimate purposes such as long-term warranty support, dispute management, or compliance.

9.5.2 Archived information is subject to appropriate access controls and security measures.

10. CUSTOMER RIGHTS AND ACCESS PROCEDURES

10.1 Right to Access Personal Information

10.1.1 You may request access to personal information we hold about you (APP 12).

10.1.2 To request access, contact our Privacy Officer using the details in **Section 20.1**.

10.1.3 We may require you to verify your identity before providing access, to ensure we do not disclose personal information to an unauthorised person.

10.1.4 We respond to access requests within a reasonable period. If we refuse access, we will provide written reasons to the extent required by the Privacy Act and advise you of complaint options.

10.1.5 We may charge a reasonable fee for providing access in some circumstances (for example, where retrieval is complex). We will inform you of any fee before proceeding.

10.2 Right to Correction

10.2.1 You may request correction of personal information we hold about you if you believe it is inaccurate, out-of-date, incomplete, irrelevant or misleading (APP 13).

10.2.2 To request correction, contact our Privacy Officer (see **Section 20.1**). We may require verification to ensure the correction is authorised.

10.2.3 If we correct information, we will take reasonable steps to notify third parties to whom we have disclosed the information if requested by you, unless it is impracticable or unlawful.

10.2.4 If we refuse to correct information, we will provide reasons and, where required, take reasonable steps to associate a statement with the information noting your request.

10.3 Right to Restrict Processing

10.3.1 You may request that we restrict certain uses of your personal information, including:

- opting out of direct marketing (see **Section 11.2**);
- limiting certain communications channels; and
- requesting human review of certain AI-influenced outcomes (see **Section 5.4**).

10.3.2 We will consider requests having regard to our legal obligations and operational requirements (for example, we may still need to use contact details to administer a building contract, provide warranty services, or comply with safety requirements).

10.4 Complaint Resolution Procedures

10.4.1 If you have a concern or complaint about how we have handled your personal information, you may contact our Privacy Officer (see **Section 20.1**).

10.4.2 Our complaint handling process is set out in **Section 18** and includes:

- acknowledging your complaint;
- investigating the issues raised;
- consulting relevant internal stakeholders and service providers as needed;
- providing a response within a reasonable timeframe; and
- implementing remedial actions where appropriate.

10.5 External Complaint Mechanisms

10.5.1 If you are not satisfied with our response, you may lodge a complaint with the OAIC. OAIC contact details are set out in **Section 20.3**.

11. MARKETING AND COMMUNICATIONS

11.1 Direct Marketing Practices

11.1.1 We may use your personal information to send direct marketing communications about our designs, products, services, events, promotions and content that may be of interest to you.

11.1.2 Direct marketing may be delivered via channels such as email, SMS, telephone, post, and digital advertising.

11.1.3 We may tailor marketing based on information about your interactions with us (for example, the types of designs you viewed or enquired about), subject to applicable laws and your preferences.

11.2 Consent and Opt-Out Mechanisms

11.2.1 We provide opt-out options in marketing communications where required, and you may opt out at any time by:

- using the unsubscribe function in an email;
- following opt-out instructions in SMS messages; or
- contacting our Privacy Officer (see **Section 20.1**).

11.2.2 If you opt out of marketing, we may still contact you for non-marketing purposes (for example, to administer your building contract, provide warranty services, or respond to enquiries).

11.3 Third-Party Marketing Partnerships

11.3.1 We may engage marketing partners to assist with campaign delivery, analytics and advertising.

11.3.2 Where personal information is disclosed to marketing partners, we take reasonable steps to ensure it is limited to what is necessary and subject to appropriate contractual controls.

11.4 Social Media and Digital Marketing

11.4.1 We may use digital marketing tools and platforms to:

- measure campaign performance;
- deliver advertisements to audiences likely to be interested in our services; and
- conduct retargeting based on interactions with our websites and content, where permitted.

11.4.2 Digital advertising platforms may use cookies and similar technologies (see **Section 12.5**). You can manage cookie preferences through browser settings and, where available, platform controls.

11.5 Customer Testimonials and Case Studies

11.5.1 We may request consent to use customer testimonials, reviews, images or project stories in marketing materials.

11.5.2 Where we use testimonials or case studies, we aim to:

- obtain consent where appropriate;
- avoid publishing unnecessary personal information; and
- respect requests to withdraw or update consent where reasonably practicable.

12. WEBSITE, MOBILE APPS, AND DIGITAL SERVICES

12.1 Website Data Collection

12.1.1 When you use our websites, we may collect personal information you submit (for example, enquiry forms and appointment requests) and information collected automatically (for example, IP address and browsing activity) as described in **Section 2.6**.

12.1.2 We use this information to:

- operate and improve our websites;
- respond to enquiries and requests;
- measure performance and improve user experience; and
- support security and fraud prevention.

12.2 Mobile Application Privacy

12.2.1 If we provide mobile applications, we may collect information necessary to provide app functionality, which may include:

- device identifiers and app usage data;
- notification preferences; and
- where enabled by you, device permissions (for example, camera access for document upload).

12.2.2 Where an app requests access to device features, you can usually control permissions through your device settings.

12.3 Online Tools and Calculators

12.3.1 We may provide online tools (for example, design configurators, cost estimators, or appointment booking tools). These tools may collect information you input and generate outputs to assist your enquiry.

12.3.2 We may store tool inputs and outputs where reasonably necessary to:

- save progress (where functionality exists);
- provide follow-up assistance; and
- improve tool performance and customer experience.

12.4 Third-Party Integrations

12.4.1 Our digital services may integrate with third-party providers (for example, analytics, customer support, and marketing automation providers).

12.4.2 Where third-party providers collect information through our digital services, their handling of information may be subject to their own terms and privacy policies, in addition to this Privacy Policy.

12.5 Digital Cookie and Tracking Policy

12.5.1 We may use cookies and similar technologies (for example, pixels and tags) to:

- remember preferences;
- enable core website functionality;
- analyse traffic and usage patterns;
- measure campaign effectiveness; and
- support advertising and retargeting where permitted.

12.5.2 Cookies may be:

- **session cookies** (which expire when you close your browser); or
- **persistent cookies** (which remain for a set period unless deleted).

12.5.3 You can manage cookies by adjusting your browser settings to refuse cookies or delete existing cookies. If you disable cookies, some website features may not function as intended.

13. SPECIAL CIRCUMSTANCES AND SENSITIVE SITUATIONS

13.1 Financial Hardship and Vulnerable Customers

13.1.1 If you disclose information indicating financial hardship or vulnerability, we handle that information with care and limit access to personnel who need it to manage your arrangements and communications.

13.1.2 We may use this information to:

- manage payment arrangements where applicable; and
- ensure communications are appropriate and responsive to your circumstances.

13.2 Deceased Customer Information

13.2.1 We may hold personal information relating to deceased customers in connection with contract administration, warranty support, or dispute management.

13.2.2 We may require evidence of authority before discussing or disclosing information to family members, executors or administrators.

13.3 Legal Proceedings and Disputes

13.3.1 We may use and disclose personal information in connection with disputes, complaints, and legal proceedings, including to:

- obtain legal advice;
- respond to claims and allegations;
- comply with court or tribunal processes; and
- preserve records relevant to actual or anticipated proceedings.

13.3.2 We may implement "litigation hold" processes to preserve relevant records where necessary.

13.4 Media and Public Relations

13.4.1 We may handle personal information in connection with public relations activities (for example, awards submissions or media content) only where appropriate and, where required, with consent.

13.4.2 We aim to avoid publishing personal information unless it is necessary and authorised.

13.5 Regulatory Investigations and Compliance

13.5.1 We may disclose personal information to regulators and authorities where required or authorised by law, including for investigations, audits, and compliance reviews.

13.5.2 We take reasonable steps to ensure disclosures are limited to what is required or authorised.

14. EMPLOYEE AND CONTRACTOR PRIVACY

14.1 Staff Privacy Training and Obligations

14.1.1 We maintain privacy and confidentiality expectations for staff and contractors who handle personal information.

14.1.2 We may provide training and guidance covering:

- privacy obligations under the Privacy Act and internal policies;
- secure handling of customer information;
- recognising and reporting privacy incidents; and
- appropriate use of systems and access credentials.

14.2 Contractor and Supplier Privacy Requirements

14.2.1 We may require contractors, subcontractors and suppliers who handle personal information to:

- use personal information only for authorised purposes;
- protect personal information with appropriate security measures; and
- notify us of suspected or actual data breaches affecting our information.

14.3 Access Controls and Permission Systems

14.3.1 We apply access controls designed to ensure personnel access only the personal information necessary for their role.

14.3.2 We may review access permissions periodically and adjust access based on role changes and operational needs.

14.4 Monitoring and Compliance Verification

14.4.1 We may monitor systems and access logs to:

- detect unauthorised access;
- investigate incidents; and
- support compliance and security.

14.4.2 Where issues are identified, we may take corrective action, including process improvements and additional training.

15. PRIVACY GOVERNANCE AND MANAGEMENT

15.1 Privacy

15.1.1 Our Legal & Risk team is responsible for coordinating privacy management, including:

- responding to privacy enquiries and access/correction requests;
- managing privacy complaints;
- supporting privacy training and awareness;
- coordinating data breach response processes; and
- supporting continuous improvement of privacy practices.

15.2 Privacy Impact Assessments

15.2.1 We may conduct privacy impact assessments for initiatives that may involve new or changed handling of personal information, including:

- new digital platforms or customer tools;
- new AI-enabled processes; and
- changes to data sharing arrangements.

15.2.2 Assessments may consider:

- the types of data involved;
- risks to individuals;
- security controls; and
- transparency and notice requirements.

15.3 Privacy by Design Implementation

15.3.1 We aim to embed privacy considerations into business processes and system design, including:

- minimising collection to what is reasonably necessary;
- applying appropriate access controls; and
- considering de-identification and retention controls.

15.4 Regular Privacy Reviews and Updates

15.4.1 We review this Privacy Policy and our privacy practices periodically and update them as required to reflect changes in our operations, systems, or legal requirements.

15.4.2 Updated versions will be made available through our usual publication channels.

16. NOTIFIABLE DATA BREACHES AND INCIDENT RESPONSE

16.1 Data Breach Identification and Assessment

16.1.1 We maintain procedures to identify and assess suspected data breaches.

16.1.2 Where a suspected breach occurs, we take steps to:

- contain the incident;
- assess what information is involved;
- assess the likelihood of serious harm; and
- determine whether notification is required under the NDB scheme.

16.2 Breach Containment and Investigation

16.2.1 Our response may include:

- securing systems and disabling compromised accounts;
- recovering information where possible;
- engaging technical specialists where appropriate;
- preserving evidence; and
- documenting findings and actions taken.

16.3 Customer and Regulatory Notification

16.3.1 If an incident is assessed as an eligible data breach, we will notify affected individuals and the OAIC as required by the Privacy Act.

16.3.2 Notifications will include the information required by the Privacy Act, including:

- the kinds of information involved; and
- recommended steps individuals should take.

16.4 Post-Breach Recovery and Improvement

16.4.1 After an incident, we may:

- remediate vulnerabilities;
- update policies and procedures;
- provide additional training; and
- review third-party arrangements where relevant.

17. CHILDREN AND FAMILY INFORMATION

17.1 Information About Minors

17.1.1 We may collect limited information about minors where it is reasonably necessary for design planning or safety management.

17.1.2 We do not knowingly collect personal information from minors directly for marketing purposes.

17.2 Family Circumstances and Household Information

17.2.1 We may collect household and family information where relevant to:

- design suitability and functionality;
- accessibility and future-proofing; and
- safety considerations for site visits.

17.2.2 We aim to collect only what is necessary and relevant to the purpose.

17.3 Educational and Safety Considerations

17.3.1 We may use family-related information to support safety communications (for example, guidance for visiting display homes or sites).

17.3.2 We do not use family information for unrelated purposes without consent or another lawful basis.

18. DISPUTE RESOLUTION AND COMPLAINTS HANDLING

18.1 Internal Complaint Procedures

18.1.1 You may lodge a privacy complaint by contacting our Customer Care Team (see **Section 20.1**).

18.1.2 To assist us to investigate, please provide:

- your name and contact details;
- a description of the complaint;
- relevant dates and reference numbers (for example, contract number, if applicable); and
- any supporting documents.

18.1.3 We will:

- acknowledge receipt within a reasonable time;
- assess and investigate the complaint; and
- provide a written response within a reasonable timeframe.

18.2 Legal & Risk Investigation Process

18.2.1 The investigation may include:

- reviewing relevant records and system logs;
- consulting relevant business units and service providers;
- assessing compliance with the Privacy Act and internal policies; and
- determining appropriate remedial actions.

18.2.2 Possible outcomes may include:

- providing explanations or information;
- correcting records;

- implementing process improvements; and
- taking steps to prevent recurrence.

18.3 External Review and Appeal Options

18.3.1 If you are not satisfied with our response, you may lodge a complaint with the OAIC (see **Section 20.3**).

18.4 Systemic Issues and Process Improvement

18.4.1 We may analyse complaints to identify systemic issues and implement broader improvements, including updates to training, procedures, and security controls.

19. POLICY UPDATES AND CHANGE MANAGEMENT

19.1 Policy Review and Update Procedures

19.1.1 We review and update this Privacy Policy as needed to reflect:

- changes to our operations, systems or services;
- changes to legal requirements; and
- improvements to privacy and security practices.

19.1.2 Updates are approved through our internal governance processes.

19.2 Customer Notification of Changes

19.2.1 We may notify customers of material changes by:

- posting the updated policy on our website(s);
- providing notices through digital channels; and/or
- other communication methods appropriate to the nature of the change.

19.3 Legacy Practice Transition

19.3.1 Where we change practices, we take reasonable steps to implement changes in a controlled manner, including updating internal procedures and communications.

19.3.2 Where a change affects how we handle personal information collected previously, we will manage the transition consistently with the Privacy Act.

20. CONTACT INFORMATION AND FURTHER ASSISTANCE

20.1 Customer Care Contact Details

You may contact our Customer Care for:

- access and correction requests;

- privacy enquiries; and
- privacy complaints.

Customer Care (Australian Building Company)
Email: PrivacyABC@abchomes.com.au
Telephone: 131 828
Post: Privacy Officer, Australian Building Company, 501 Blackburn Road, Mt Waverley, Victoria

20.2 General Privacy Inquiries

20.2.1 For general privacy enquiries, you may contact Customer Care using the details in **Section 20.1**.

20.2.2 We aim to respond within a reasonable timeframe, noting that response times may vary depending on complexity and verification requirements.

20.3 External Regulatory Contacts

If you wish to contact the OAIC:

Office of the Australian Information Commissioner (OAIC)
Website: https://www.oaic.gov.au
Telephone: 1300 363 992
Post: GPO Box 5218, Sydney NSW 2001, Australia

20.4 Emergency Privacy Contacts

20.4.1 If you believe there is an urgent privacy or security issue (for example, suspected unauthorised access to your information in connection with our services), contact our Customer Care using the details in **Section 20.1** and mark your communication as **Urgent: Privacy Incident**.

20.4.2 We will triage urgent matters as quickly as reasonably practicable.