

Privacy Policy

Bookallil Limited, trading as Bookallil Advisory

Privacy Policy · Governance Document · MASTER

Issued 22 August 2026

Effective Date: 22 August 2026

Document Status	Governance Document
Document Version	MASTER
Issue Date	22 August 2026
Effective Date	22 August 2026
Owner	Martin Bookallil, Principal Advisor and Founder
Approved By	Martin Bookallil, Principal Advisor and Founder
Review Date	22 August 2027
Document Classification	Public

Bookallil Limited, trading as Bookallil Advisory (“Bookallil Advisory”, “BA”, “we”, “our” or “us”) respects your privacy. This Privacy Policy explains how we collect, use, share, store and protect personal information across our website and our advisory business, including our work with clients, contractors, representatives, partners and the customers and prospects introduced into opportunities we manage.

In this Policy, “personal information” means information from which a living individual can be identified, whether directly or together with other information we hold. It includes what some laws call “personal data”.

1. Scope and Status of this Policy

This Policy applies when you:

- Visit our website
- Contact us or make an enquiry
- Are, or may become, a client, prospect or business contact
- Participate in an advisory project or engagement
- Are introduced into an opportunity that BA manages
- Apply to become, or act as, a contractor, representative, partner or other BA participant
- Use, or are recorded in, BA systems
- Take part in a Deal, commission, payment or onboarding process
- Communicate with us by email, meeting, messaging, form or other business channel

BA is a “data user” under the Hong Kong Personal Data (Privacy) Ordinance, Cap. 486. Under other privacy laws that may apply to a particular activity, BA may be described as a controller.

Our privacy role is not the same for everything we do. Depending on the system, the contract and the specific activity, BA may determine how personal information is handled, may handle it on behalf of a client or counterparty, or may share responsibility with another organisation. We do not claim to be the controller, or the processor, for every activity described here.

We may also give you a separate Personal Information Collection Statement or notice at the point where information is collected, for example on a form, survey, onboarding process or transaction. This Policy does not replace a collection notice that is legally required in that situation.

2. BA Systems, the BA CRM and Enerzyz Systems

BA works in partnership with Enerzyz. Because personal information can sit in more than one system, it helps to be clear about which is which.

The BA CRM is BA's own system and our controlling internal record for Deal registration, Deal ownership, internal registration timestamps, participants, lead classification, Helpers, Chain Owners, BA Partner Governance Support allocations, activity history and commission administration.

Certain facility-assessment records handled by BA, including utility bills, site photographs, facility information and related supporting documents, are currently stored in a BA-dedicated cloud environment in India. BA's current system documentation identifies this environment as the Amazon Web Services Asia Pacific (Mumbai) Region (ap-south-1). BA's primary application infrastructure is hosted separately, in Singapore. Uploaded documents, videos and other BA assets are stored in the India environment. These records are encrypted in transit and at rest. Access is limited to authorised personnel and service providers who require it for the relevant assessment, customer engagement, security, support or administration purpose.

For its internal CRM, business-development and administration activities, BA generally determines why and how personal information is handled. When BA handles facility or customer information on behalf of Enerzyz, a customer or another contracting party, BA may instead act as a service provider, processor or subprocessor under the applicable contract. In particular, where BA operates the facility assessment survey offered in connection with Enerzyz onboarding, BA acts as a subprocessor engaged by Enerzyz, and handles the uploaded documents only for the purpose of conducting that assessment and preparing its outputs. BA's role therefore depends on the relevant information, system and activity.

The Enerzyz DMS is the upstream record used for BA's deal protection and for administering opportunities with Enerzyz. Registering an opportunity there is separate from BA's internal record-keeping.

The Enerzyz DMS and platform are separate from BA's internal CRM and BA-dedicated document environment. Under the applicable customer contracts and data-processing arrangements, information handled through Enerzyz systems may be hosted or processed in Singapore, the United States or another agreed location.

This Policy describes how BA handles personal information. It does not replace Enerzyz's own privacy policy, a customer contract, or any data-processing agreement that governs the Enerzyz platform or DMS.

3. Personal Information We Collect

We collect only what we reasonably need. The categories below will not all apply to every person.

A. Contact and professional information

- Name
- Employer or business
- Job title and role
- Business email address
- Telephone and messaging details
- Country, market and business address
- Professional profile and relevant experience

B. Enquiry, client and project information

- Enquiries and contact-form submissions
- Proposals and engagement records
- Meeting notes and communications
- Project requirements, deliverables and correspondence
- Customer and prospect contacts
- Facility, property or opportunity information, where it relates to an identifiable person
- Facility-assessment responses, energy and utility information, building and equipment information, utility bills, site photographs, videos and related supporting documents, including any limited personal information contained in those materials

C. Contractor, partner and representative information

- Contact and entity details
- Assigned role, tier, market or territory
- Qualifications and experience
- Onboarding and training completion
- Insurance and compliance information
- Conflict-of-interest declarations
- Code-of-conduct and policy acknowledgements
- Suitability, activity and performance records
- System permissions and access history

D. Identity-verification information

- Identity-verification status
- The type of document checked
- The verification date and verifier
- Government-issued identification details or copies, only where legally required or reasonably necessary

Wherever practical, we record that identity has been verified rather than keeping a copy of the identity document itself. An authorised local sponsor, contracting partner or service provider may carry out the verification and give us the result. A copy of the document should not be passed to or kept by BA unless it is necessary for a lawful purpose.

E. Deal, CRM and commercial information

- BA CRM registration timestamp
- Deal Owner and originating participant
- Helpers, Chain Owners and other approved allocations
- Lead source and classification
- Opportunity status and activity history
- Customer and prospect contacts
- Proposals and transaction records
- Commission eligibility, calculations, statements and disputes

F. Financial, payment and tax information

- Invoice and payment details
- Bank-account information

- Tax residency and tax documentation
- Commission and expense records
- Payment history

G. Technical and security information

- IP address
- Browser, device and operating-system information
- Login and system-access records
- Security and audit logs
- Cookie and analytics information
- Records of suspected misuse or security incidents

H. Facility assessments and restricted information

BA's facility assessment services are intended to collect building, plant, equipment, utility and operational information required for an assessment. Unless expressly agreed otherwise in writing, these services are not designed to collect patient or clinical information, health records, hotel guest or customer profiles, payment-card information, government identification documents, biometric information or other sensitive personal information. You should not submit such information through a facility assessment form or document-upload function. If you believe a document necessary for an assessment contains this information, please contact BA before uploading it.

We seek to avoid collecting sensitive or unnecessary personal information. Where sensitive information is collected at all, we do so only where it is lawful and reasonably necessary for a specific purpose.

You are not obliged to give us personal information, but some services or roles may not be available if you choose not to.

4. Where We Obtain Information

We may obtain personal information from:

- You directly
- Your employer or business
- A BA contractor, representative, partner or authorised sponsor
- A customer or prospective customer
- Enerzyz or another Solution Provider
- The BA CRM, the Enerzyz DMS and other authorised systems
- Meetings, correspondence and business communications
- Public professional or corporate sources
- Service providers used for verification, payments, communications or system administration

We will not collect personal information by unlawful or unfair means.

5. How We Use Personal Information

We use personal information to:

- Respond to enquiries
- Provide advisory and consulting services

- Prepare proposals and manage engagements
- Conduct facility assessments, evaluate suitability for relevant services, and prepare assessment reports, recommendations and related outputs
- Manage client and prospect relationships
- Register, assign and progress Deals
- Establish internal BA Deal ownership
- Register opportunities upstream where required
- Manage contractors, partners and representatives
- Carry out onboarding, suitability, compliance and identity checks
- Administer system access
- Calculate and pay commissions and expenses
- Maintain financial, tax and audit records
- Resolve Deal-ownership or commission disputes
- Protect BA, its clients, systems and confidential information
- Detect misuse, fraud or security incidents
- Meet contractual, legal and regulatory requirements
- Improve our website, services and operations
- Send business communications and direct marketing where lawfully permitted

We will not use your personal information for a new and unrelated purpose without your prescribed consent where applicable law requires it.

6. Our Basis and Authority for Handling Personal Information

Privacy laws differ between jurisdictions, and the lawful basis for handling information depends on where you are and what we are doing. In general, we handle personal information where:

- It is necessary to respond to your request or to perform a contract
- It is directly related to BA's lawful business activities and to the purpose for which it was collected
- You have given consent, where consent is required
- We must comply with a legal or regulatory requirement
- It is reasonably necessary to protect BA's systems, rights or legitimate business operations, subject to applicable law
- Another lawful basis or exemption applies in the relevant jurisdiction

7. Direct Marketing and Business Communications

We may send you relevant business information, but only where applicable law permits it.

Where the Hong Kong Personal Data (Privacy) Ordinance applies, before we use your personal data for direct marketing we will notify you:

- That we intend to use your personal data for direct marketing, and that we may not do so without your consent or an indication of no objection
- Of the kinds of personal data that will be used
- Of the classes of BA services or business subjects that may be promoted
- Of the response channel through which you may give consent or indicate no objection

We will not begin that direct marketing unless we have received the required consent or indication of no objection. Silence, non-response or a failure to opt out does not amount to consent or to an indication of no objection.

You may require us to stop using your personal data for direct marketing at any time and without charge. We will act on that request and keep an appropriate suppression record.

Marketing communications will identify BA as the sender.

Operational, contractual, security, onboarding, commission and Deal-related messages are not marketing. We may still need to send those to you even if you have opted out of marketing, and Hong Kong law does not require consent for ordinary business communications of that kind.

8. Sharing and Disclosure

We share personal information only to the extent reasonably necessary, and only with:

- BA personnel, contractors and authorised representatives
- BA's authorised developers, technology-support providers and security providers
- Cloud hosting, backup and infrastructure providers
- Customers and prospective customers involved in the relevant matter
- Enerzyz and other Solution Providers, where required for the relevant opportunity, assessment or service
- Authorised country partners, sponsors and Deal participants
- CRM, email, communications, e-signature, analytics and IT-security providers
- Identity-verification and onboarding providers
- Banks, payment providers, accountants, auditors, insurers and tax advisers
- Lawyers and other professional advisers
- Regulators, courts, law-enforcement authorities and government bodies
- A purchaser, investor or successor in a genuine corporate transaction, subject to appropriate confidentiality protection

In each case, access must be limited to what the relevant purpose requires, and is subject to appropriate confidentiality, contractual and security requirements.

We do not sell or rent personal information, and we do not trade it for advertising purposes.

The legal role of each recipient depends on the activity and the contract. Some act on our instructions; others handle information in their own right or under their own legal obligations. We do not describe every third party as a processor.

9. International Storage and Transfers

Personal information may be accessed, stored or otherwise processed in Hong Kong, Australia, India, Singapore, the United States and other jurisdictions used by BA or its approved service providers. The location depends on the relevant system, service and activity.

BA's primary application infrastructure is currently hosted in Singapore. Uploaded documents, videos and other BA assets, including facility-assessment records such as utility bills, site photographs, facility information and related supporting documents, are stored in a BA-dedicated cloud environment in India, documented as the Amazon Web Services Asia Pacific (Mumbai) Region (ap-south-1). Automatic daily server backups, and additional server snapshots, are maintained in the relevant hosting region.

Where applicable customer contracts and data-processing arrangements apply, information handled through the Enerzyz DMS or platform may be processed in Singapore, the United States or another agreed hosting location.

Authorised personnel and service providers may access information from the country in which they perform their responsibilities. BA applies contractual, organisational and technical safeguards appropriate to the information, processing activity, recipient and destination involved.

Privacy laws differ between jurisdictions and may offer different levels of protection. We remain responsible for our own handling of personal information, and we require relevant providers to protect it consistently with their role and with applicable law.

10. How Long We Keep Information

How long we keep personal information depends on what it is and why we hold it.

- Enquiry and prospect information is kept only while reasonably required for follow-up, relationship management or legitimate record-keeping
- Active client, contractor, Deal and project records are kept for the duration of the relationship and for a reasonable period afterwards
- Financial, tax, transaction, payment and commission records may be kept for at least seven years, where Hong Kong law requires it
- Security, access and incident records are kept according to risk, investigation needs and legal requirements
- Copies of identity documents should be deleted once no longer required; a record that verification took place may be kept for compliance and audit purposes
- A litigation hold, regulatory requirement or unresolved dispute may require us to keep information for longer
- Assessment records and uploaded documents are retained only for the applicable customer, contractual, operational, evidentiary or legal purpose
- Records are deleted, anonymised or placed beyond ordinary use when no longer required
- Deletion from active systems may occur before deletion from protected backups. Backup copies remain access-restricted and are deleted or overwritten in accordance with BA's applicable backup-retention procedures.

When information is no longer required, we securely delete, destroy or anonymise it.

11. Security

We apply security controls proportionate to the sensitivity of the information and the risk involved, including:

- Role-based access
- Authentication and access controls
- Encryption in transit and at rest where supported and appropriate
- System logging and monitoring
- Automatic daily backups, server snapshots and recovery controls
- Confidentiality obligations on personnel and contractors
- Vendor review and service-provider controls
- Security review and incident-response processes
- Data minimisation

No method of transmission over the internet, and no method of electronic storage, is completely secure. While we take reasonable steps to protect personal information, we cannot guarantee absolute security.

Customers conducting privacy or security due diligence may contact BA for further information about the controls applicable to the relevant BA service, subject to appropriate confidentiality arrangements.

12. Artificial Intelligence

BA uses approved AI-enabled tools to support its work, for example in research and analysis, drafting and summarisation, meeting-note preparation, administrative assistance, CRM support and operational reporting.

Where we use these tools, we:

- Limit the personal information entered into AI systems
- Use anonymised or pseudonymised information where practical
- Avoid entering identity documents, sensitive personal information or confidential customer information into public consumer AI tools
- Apply human review to material outputs
- Apply access and security controls
- Assess the provider's privacy settings and terms, and the intended use, proportionately
- Use personal information only for the original purpose, or a directly related purpose we have disclosed, unless further consent is obtained where required

BA does not make decisions producing legal or similarly significant effects about individuals solely through automated AI processing.

The way an AI provider handles information is governed by that provider's own terms. We select tools with that in mind, but this Policy does not make representations about a third-party provider's retention or use of information.

13. Cookies, Analytics and Third-Party Links

Our website may use cookies and similar technologies. Broadly, these fall into the following categories:

- Strictly necessary cookies, which enable core site functions and cannot usefully be switched off
- Functional cookies, which remember preferences and improve how the site works
- Analytics cookies, which help us understand how the site is used, and which may collect device and usage information such as IP address, browser type and pages visited

You can manage or disable cookies through your browser settings, although some features may not work correctly if you do. Where applicable law requires consent for non-essential cookies, we will ask for it before those cookies are set.

Our website may link to third-party websites. Those sites operate under their own privacy policies, and we are not responsible for their content or privacy practices.

14. If Something Goes Wrong: Data-Breach Response

If we suspect a personal-data incident, we will:

- Investigate promptly

- Take reasonable containment and remediation measures
- Assess the nature of the information involved and the risk of harm to affected individuals
- Notify affected individuals, regulators, clients or other relevant parties where legally required or reasonably appropriate
- Cooperate with applicable service providers and contractual counterparties

In Hong Kong, timely notification to the Privacy Commissioner for Personal Data is encouraged as good practice rather than mandatory in every case. Where another jurisdiction imposes a mandatory notification requirement, or a contract requires notification, we will comply with it.

Separately from any regulatory position, BA will notify an affected customer or contracting party without undue delay where notification is required by the applicable contract or law, or where the assessed risk makes notification appropriate.

15. Your Rights

Subject to applicable law, you may:

- Ask whether we hold personal information about you
- Request access to that information
- Request correction of information that is inaccurate
- Request deletion, where a legal right to deletion applies
- Object to or restrict certain uses, where that right applies
- Withdraw consent, where our handling relies on consent
- Opt out of direct marketing
- Make a privacy complaint

Under the Hong Kong Personal Data (Privacy) Ordinance, the core rights are the right to request access to your personal data and the right to request correction of inaccurate data. Rights to deletion, restriction and objection are not general rights in Hong Kong; they may nevertheless be available to you where another jurisdiction's law applies to the handling in question.

In responding to a request, we may:

- Verify your identity
- Ask for enough detail to locate the information
- Refuse or limit a request where the law permits
- Charge a fee for an access request, only where legally permitted and not excessive
- Retain information where required by law, by contract, for legal claims, or for legitimate compliance obligations

If you are not satisfied with our response, you may complain to the relevant privacy regulator. In Hong Kong that is the Office of the Privacy Commissioner for Personal Data.

16. Children

Our website and services are directed to businesses and professionals. They are not intended for children, and we do not knowingly seek to collect children's personal information.

17. Changes to this Policy

We may update this Policy from time to time. Where a change is material, we will publish the updated Policy with a revised effective date. Please check this page for the current version.

18. Contact Us

If you have a question about this Policy or about how we handle personal information, or if you wish to make an access or correction request or a privacy complaint, please contact Martin Bookallil:

Privacy enquiries, questions about where information is held, and customer security due-diligence requests may all be directed to the same contact.

Entity	Bookallil Limited, trading as Bookallil Advisory
Company Number	3216366
Address	9th Floor, Amtel Building, 148 Des Voeux Road Central, Hong Kong
Privacy Contact	Martin Bookallil, Principal Advisor and Founder
Email	martin@bookalliladvisory.com
Telephone / WhatsApp	+852 9153 9508
Website	bookalliladvisory.com