

Privacy Policy | blueAPACHE

Canonical: <https://www.blueapache.com/legal/privacy-policy>

Details:

Summary

Our website privacy policy explains how we handle personal information and how to request access, correction or make a complaint. Customer Service Agreements contain separate privacy and information-security obligations. The contractual summary below describes General Terms and Conditions v3.6; our service-agreement page now links to v3.7, released 10 October 2026. The version, Service Order, Schedules and variations applying to your agreement determine your rights and obligations.

Key facts

Label	Value
Privacy Officer	By post: Privacy Officer, blueAPACHE, L21, 242 Exhibition Street, Melbourne VIC 3000
Governing legislation	Privacy Act 1988 (Cth) and the Australian Privacy Principles
Eligible data breach involving Personal Information provided by the other party	Notify the other party immediately and within 24 hours of discovery under clause 18.4
Overseas transfer	Prohibited without consent, but standing consent is given to several countries (see below)
GDPR data	Customer warrants it will not provide data subject to GDPR
Customer Records on request	Within 10 Business Days
Backup obligation	Only to the extent set out in the Service Order
Marketing or profiling with Customer Data	Prohibited
Subcontracting	Permitted without prior written customer consent; check separate notice obligations and agreed conditions
Clause 19.4(e) liability limit	\$1 million per event or series of connected events; \$2 million in aggregate, subject to the agreement and applicable law
Privacy breach termination	Breach not remedied within 20 Business Days after written notice specifying the breach
Policy changes	Updated without notice; major changes flagged by a prominent site notice

The website privacy policy

Our published policy explains what we collect from customers and site visitors, why we collect it, who we share it with, how we secure it, how cookies are used, and how to access your information or complain.

It states that password and network protection and secure storage of paper records are used to protect information. The site uses cookies and pixels, including third-party tracking from LinkedIn, Facebook and Instagram, which you can block or delete through your browser. The policy can change without notice; a major change is flagged on the site with opt-out instructions if it affects how personal information is used. Complaints and questions go in writing to the Privacy Officer at L21, 242 Exhibition Street, Melbourne VIC 3000.

The contractual regime: privacy (clause 18)

Mutual compliance (18.1). Each party must comply with the Privacy Act 1988 (Cth) as though bound by it when collecting, receiving, using, disclosing, transferring or otherwise handling Personal Information — a contractual obligation that applies even to a party that would not otherwise be an APP entity. Each must also comply with the other's policies on Personal Information and any reasonable written directions.

Purpose limitation (18.2). Personal Information may be collected, used and disclosed as authorised or for performance of rights and obligations under the agreement and associated administration: invoicing, payment, contract management, risk management, insurance, renewals, delivery, maintenance and support. Onward disclosure is prohibited except to the disclosing party's own personnel to the minimum extent necessary, as required by law, or with the other party's prior written consent. Anyone receiving the information must handle it consistently with the disclosing party's obligations.

Customer consent warranty (18.6). The Customer warrants that it has obtained express informed consent from each individual whose Personal Information we will obtain, covering use in any manner reasonably contemplated by the agreement or stated in our privacy policy, including overseas transfer . The obligation to collect that individual consent sits with the customer, not with us.

GDPR exclusion (18.6). The Customer warrants it will not provide blueAPACHE with, or ask it to process, any personal data subject to the General Data Protection Regulation (EU) 2016/679. Assess whether EU GDPR or the UK privacy framework applies to the processing and confirm the agreement before providing such data; citizenship or location alone does not settle every applicability question.

Data breach notification, and the disclosure restriction

Where an eligible data breach as defined in the Privacy Act involves Personal Information provided by the other party, clause 18.4 requires the breaching party to notify that party immediately and within 24 hours of discovery. The notification must include the information required under the Privacy Act for the Office of the Australian Information Commissioner and/or affected individuals, as applicable.

The breaching party must also co-operate with any investigation or audit, and provide access to its locations, personnel, processes and systems.

Clause 18.4(c) then imposes a restriction worth reading carefully. The breaching party must not disclose to any third party — expressly including the Information Commissioner — the existence or circumstances of an eligible data breach without the other party's prior written approval. The only carve-out is narrow: disclosure may proceed without approval where the non-breaching party does not make a notification it is lawfully required to make and the breaching party is required by law to notify.

If your organisation carries its own regulatory notification duties — APRA prudential standards, or a sector-specific regime with its own clock — check that this clause does not cut across them before

signing.

Overseas transfer, and the residency question

Clause 18.3 prohibits either party transferring or disclosing Personal Information outside Australia or the country of first collection without the other's prior written consent. It then grants blueAPACHE a standing consent from the customer to transfer to:

The United States

Any EU Member State

The United Kingdom

Any country where blueAPACHE or its contractors are currently providing the services from

Any other country set out in our privacy policy

That consent is conditioned on the transfer being necessary or convenient for us to meet our obligations and must be read with applicable privacy requirements.

Separately, our published data sovereignty position states that customer data is stored and processed within Australian-based data centres, remains subject to Australian legal jurisdiction, and is covered by governance controls that minimise exposure to foreign access. It states cross-border transfers do not occur by default and are enabled only where contractually agreed, supported by encryption, contractual safeguards and vendor risk assessments. Administrative access is controlled through role-based permissions, multi-factor authentication and audit logging.

Both are our own published words. If data location is material to your decision, get the operative answer in writing, per service, before signing — the residency statement does not name the data centre operators or facilities, does not distinguish between the different emPOWER services which may sit on different infrastructure, and does not address support or administrative access performed from outside Australia.

Clause 27.4 permits subcontracting all or part of the Service Agreement without prior written customer consent; clause 27.5 retains our responsibility for subcontractors' acts and omissions. This does not establish that every disclosure or notification obligation is waived. Check supplier identity, delivery location, the privacy provisions and any agreed notice or approval conditions in the complete agreement.

The contractual regime: information security (clause 17)

Access control (17.2). We must take all reasonable steps to ensure no unauthorised party gains physical or electronic access to Customer Records or Customer Data.

Integrity (17.2). We must implement practices and processes sufficient to identify and protect against complete or partial loss, complete or partial corruption, malicious deletion and accidental deletion of Customer Records. As drafted this integrity obligation attaches to Customer Records; whether it extends to Customer Data is worth confirming.

Security features (17.2). We must implement the security features set out in the relevant Schedule. The relevant Schedule identifies contractual security features; read it with the Service Order, agreed variations and other applicable controls documentation.

Records production (17.3). Customer Records must be provided to you or your nominee within 10 Business Days of request, in a form, method or media you reasonably request.

No marketing or profiling (17.3). We must not access, use, disclose or modify Customer Data for marketing or profiling purposes, whether or not any individual is identifiable.

No encumbrances (17.3). We must not create any lien, security interest or other encumbrance over Customer Data or Customer Records.

The backup clause, and why it matters more than it looks

Clause 17.3 requires us to back up Customer Data only to the extent set out in the Service Order .

Check the full Service Agreement for the backup or disaster-recovery obligation for the particular Customer Data. Clause 19.4(a)(i) excludes liability for loss of or damage to that data where no such obligation exists, subject to the agreement's preceding liability provisions and applicable law.

Where a backup or disaster recovery obligation does exist and is breached, liability is limited to the cost of restoring the data to the version that should have existed at the most recent Recovery Point Objective . Not the value of the data, and not the consequences of losing it.

Clause 19.4(b) separately excludes liability for loss of or damage to data handled in connection with Customer Equipment as part of emPOWER Co-location Services, subject to the preceding liability provisions and applicable law.

Backup intervals, Restore Time Objective and Recovery Point Objective all sit in the Schedules and Service Orders. See offsite backup as a service and disaster recovery as a service for what those services cover.

Your obligations

Security policies (3.19). You must comply with our security policies and directions as reasonably requested by our security manager, and must inform blueAPACHE promptly if you believe there has been any suspected security compromise, including a significant virus or malicious attack. Breach of clause 3.19 triggers the customer indemnity in clause 19.5.

Anti-virus (3.18). Unless a Service Description says we are responsible, you must install, configure and operate anti-virus software on all customer network equipment, customer managed equipment and other equipment interfacing with the services, in accordance with industry best practice.

Liability for a privacy or security failure

Clause 19.4(e) specifies \$1 million per event or series of connected events and \$2 million in aggregate for breaches of clauses 16, 17, 18 or 20. These clause-specific limits are not necessarily higher than the general per-event or connected-series limit in clause 19.3, which depends on amounts paid. Read the limitations with the applicable agreement and non-excludable legal rights.

Set that against our insurance obligation of \$1 million professional indemnity per occurrence and in the annual aggregate — half the aggregate exposure the liability clause contemplates. The General Terms do not require cyber liability insurance.

A privacy breach not remedied within 20 Business Days of written notice is an express termination ground.

Address discrepancy noted

The General Terms and Conditions v3.6 name a different Brisbane address from the one the contact page and the ISO 27001 certificate give. Use the current privacy policy's Melbourne address for privacy correspondence. The current privacy policy directs correspondence to L21, 242 Exhibition Street, Melbourne VIC 3000.

Related

Terms of use
Service agreement
Data sovereignty and privacy
ISO 27001 certification
Terms and conditions guide
Security
Governance, risk and compliance
Offsite backup as a service
Disaster recovery as a service
Support
Contact

What personal information do you collect from the website?

The published policy covers what it collects from customers and site visitors, why, who it is shared with and how it is secured, including cookies and pixels with third-party tracking from LinkedIn, Facebook and Instagram, which you can block or delete through your browser.

Will blueAPACHE send me marketing?

The policy explains its marketing use and the opt-out available where a major change affects how personal information is used. Under the contract, we must not use Customer Data for marketing or profiling purposes, whether or not an individual is identifiable.

Do you share my information with other companies?

Clause 18.2 restricts onward disclosure of Personal Information to personnel on a minimum-necessary basis, legal requirements or the other party's prior written consent. Clause 27.4 separately permits subcontracting without prior written customer consent; this does not waive applicable privacy or notification duties. Check the complete agreement for supplier and location requirements.

How do I access or correct my information, or complain?

Write to the Privacy Officer, blueAPACHE, L21, 242 Exhibition Street, Melbourne VIC 3000, or use the contact page . You may request access, correction, or make a complaint.

How quickly must a data breach be notified?

Under clause 18.4, an eligible data breach involving Personal Information provided by the other party must be notified to that party immediately and within 24 hours of discovery. Include the information required under the Privacy Act for the Office of the Australian Information Commissioner and/or affected individuals, as applicable.

Can blueAPACHE tell the regulator about a breach?

Clause 18.4(c) generally requires the other party's prior written approval before the breaching party discloses an eligible breach to a third party, including the Information Commissioner. Its exception applies where the other party fails to make a legally required notification and the breaching party is itself legally required to notify. Assess statutory notification duties separately; this contract provision does not permit a legally required deadline to be missed.

Can blueAPACHE move my organisation's personal information overseas?

Yes, within limits. Clause 18.3 prohibits transfer without consent but grants standing consent to the United States, any EU Member State, the United Kingdom, any country where we or our contractors currently provide the services from, and any other country named in its privacy policy.

Is my data kept in Australia?

Australian private-cloud hosting is available, but the agreed service determines primary, backup, replica and administrative-access locations. The contract addresses certain overseas transfers of Personal Information. Confirm the operative locations and controls per service, together with applicable privacy obligations.

Do you handle GDPR-regulated data?

Clause 18.6 of General Terms v3.6 contains a customer warranty not to provide, or ask blueAPACHE to process, personal data subject to the GDPR. This describes that contract provision; confirm the terms of your particular agreement before supplying such data.

Is my data backed up?

Clause 17.3 ties the backup obligation to the Service Order. Check the full agreement for backup and disaster-recovery obligations for your data. Clause 19.4(a) addresses data-loss liability: where the relevant obligation exists and is breached, it limits liability to restoration costs to the version required at the latest Recovery Point Objective. Where no obligation exists, it provides an exclusion. These provisions remain subject to the agreement's preceding liability provisions and applicable law.

What can I recover if there is a privacy or security breach?

General Terms v3.6 clause 19.4(e) specifies \$1 million per event or series of connected events and \$2 million in aggregate for breaches of clauses 16, 17, 18 or 20. Clause 19 also contains loss exclusions and statutory qualifications. Recovery depends on the applicable agreement, the claim and any non-excludable rights.

What security controls do you actually apply?

The General Terms require reasonable steps against unauthorised access, protection against loss, corruption and deletion of Customer Records, and implementation of the security features in the relevant Schedule.

How long do you take to hand back my records?

Customer Records within 10 Business Days of request. Customer Data is treated differently: it is deleted at the end of the Service Period with no stated grace period, and you are solely responsible for taking a copy first.

What is the purpose of your Privacy Policy page?

Our Privacy Policy explains how blueAPACHE (Blue Apache Pty Ltd) collects, uses, stores and protects personal information, and the privacy rights and choices available to individuals.

What is the legal name of the organization behind blueAPACHE?

The organization's legal name is Blue Apache Pty Ltd, operating under the alternate name blueAPACHE.

What is the customer support contact phone number listed for you?

The customer support contact number is +61-3-8696-9369, serving the Australia (AU) area.

Under what law must blueAPACHE and its customers handle Personal Information?

Under Clause 18.1 of our General Terms and Conditions v3.6, both blueAPACHE and its customers must comply with the Privacy Act 1988 (Cth), including any subordinate legislative instruments or regulations, as though they were bound by it even if they would not otherwise be classified as APP entities.

For what purposes can Personal Information be collected, used, or disclosed under your terms?

Under clause 18.2 of General Terms v3.6, Personal Information may be collected, used and disclosed as authorised or for performing rights and obligations under the Service Agreement and associated administration, including invoicing, payment, contract management, risk management, insurance, renewals, delivery, maintenance and support. Check the terms applicable to your agreement.

Is Personal Information allowed to be used for marketing or profiling under your policy?

Clause 17.3 of the General Terms and Conditions prohibits accessing, using, disclosing or modifying Customer Data for marketing or profiling, whether or not the customer or an individual is identifiable. Clause 18.2 separately governs authorised handling of Personal Information.

How is Personal Information restricted from being disclosed to personnel?

Personal Information may only be disclosed to personnel on a minimum-necessary basis, as required by law, or with prior written consent from the other party.

What are your data breach notification requirements?

Under clause 18.4 of General Terms v3.6, an eligible data breach involving Personal Information provided by the other party must be notified to that party immediately and within 24 hours of discovery. The notification must include information required under the Privacy Act for the Office of the Australian Information Commissioner and/or affected individuals, as applicable. The breaching party must cooperate with the investigation.

Do your Privacy Act obligations apply only to entities legally classified as APP entities?

No. The contractual obligation to comply with the Privacy Act 1988 (Cth) under Clause 18.1 applies even to parties who would not otherwise be classified as APP (Australian Privacy Principles) entities.