Attekus

# Privacy Policy

attekus.com.au

# Privacy Policy

This Privacy Policy explains how Attekus collects, holds, uses, discloses and otherwise processes personal information. "Attekus", "we", "us" and "our" mean Attekus Pty Ltd (ABN 47 677 290 489), Attekus NZ Limited (company number 9200360), Attekus UK Limited (company number 16753136), and any related Attekus entity identified in your contract, the relevant service or a collection notice.

The Attekus entity that contracts with you, provides the relevant service or issues the collection notice is responsible for the personal information it controls. Attekus Pty Ltd is the primary contact for Australian and New Zealand operations. Attekus UK Limited is the contact for United Kingdom operations.

This policy is intended to comply, as applicable, with the *Australian Privacy Act 1988 (Cth)* and the Australian Privacy Principles; the *New Zealand Privacy Act 2020* and its Information Privacy Principles, including IPP 3A; the UK GDPR, the *Data Protection Act 2018*, the *Data (Use and Access) Act 2025* and the Privacy and Electronic Communications Regulations.

In this policy, "personal information" includes "personal data" under UK law.

## When Attekus is a controller and when it is a processor

Attekus is a controller (or agency under Australian and New Zealand law) when it determines why and how personal information is handled, including information about website visitors, business contacts, customer administrators, suppliers, applicants and people who contact us.

When an Attekus customer, such as a council, government body, education provider, event management or other organisation, uses the Attekus solution to collect or manage personal information ("**Customer Data**"), that customer generally determines the purposes and means of processing. The customer is the controller or responsible agency, and Attekus acts as its processor or service provider under the customer contract and documented instructions.

If your information was entered into an Attekus service by an Attekus customer, you should normally direct privacy requests to that customer. Attekus will assist the customer as required by law and contract. The customer's privacy notice applies to the customer's collection and use of Customer Data.

## Personal information we collect

Depending on your relationship with us and the relevant service, we may collect:

- Identity and contact information: names, email addresses, telephone numbers, postal addresses and other contact details;
- Account information: usernames, authentication details, permissions, account preferences and account activity;
- Business and professional information: employer or organisation, job title, role, professional contact details and business relationship history;
- Transaction and payment information: order, subscription, invoice, booking, registration, ticketing and payment status information. Card details are handled by PCI-compliant third-party payment providers; Attekus generally receives limited payment and transaction confirmation information;
- Communications and user content: enquiries, support requests, feedback, survey responses, correspondence and other content you submit;
- Technical and usage information: IP address, device and browser type, operating system, referring URL, cookie or similar identifiers, server logs, access dates and times, and interactions with our website and services;
- Marketing and preference information: communication preferences, event interests and responses to campaigns;
- Recruitment information: application, employment history, qualifications, references, right-to-work information and other information provided during recruitment; and
- Customer Data: information processed in the Attekus solution on behalf of a customer, which may include information about bookings, events, registrations, appointments, payments and customer interactions.

## How we collect personal information

We may collect personal information:

- directly from you when you visit our website, create or administer an account, use a service, make an enquiry, attend an event, apply for a role or communicate with us;
- from an Attekus customer or another authorised solution user when they create an account, booking, registration or record for you;
- through integrations configured by a customer, including finance, calendar, identity, payment and customer-management systems;
- from service providers, payment providers, business partners, referral partners and related Attekus entities; and
- from public sources, including professional directories, government registers, websites and professional networking platforms, where lawful.

If New Zealand law applies and we collect personal information indirectly, we will take reasonable steps to make the individual aware of the collection and the matters required by IPP 3A as soon as reasonably practicable, unless an exception applies. Where required, a collection notice may also explain the source of the information, the authority for collection, the intended recipients and the consequences (if any) of not providing information. We provide equivalent information for indirect collection under UK law where required.

## If you do not provide information

You may choose not to provide personal information unless it is required by law or needed for the requested service. If you do not provide required information, we may be unable to create or secure an account, process a transaction, provide support, consider an application or deliver the relevant service. Optional fields will be identified where reasonably practicable. You may interact with us anonymously or using a pseudonym where lawful and practicable.

## How and why we use personal information

We use personal information only for notified purposes, related purposes that an individual would reasonably expect, purposes authorised by consent, or as otherwise permitted or required by law.

For processing governed by the UK GDPR, the principal purposes and lawful bases are:

| Purpose | UK GDPR lawful basis |
|---|---|
| Provide and administer products and services, accounts, transactions, onboarding, implementation and support | Performance of a contract or steps requested before entering a contract; legitimate interests in serving an organisation and its authorised users; legal obligations where applicable |
| Authenticate users, maintain security, prevent fraud and misuse, investigate incidents and protect rights | Legitimate interests in secure and reliable services; legal obligations where applicable |
| Operate, analyse, test and improve our website, products and services | Legitimate interests in improving performance and user experience; consent where required for non-essential cookies or similar technologies |

| Purpose | UK GDPR lawful basis |
|---|---|
| Manage business relationships, respond to enquiries and send service or business communications | Performance of a contract; legitimate interests in relationship management; consent where required |
| Provide relevant marketing and event information | Consent where required; otherwise legitimate interests, subject to applicable direct-marketing and electronic-communications laws and your right to opt out |
| Billing, finance, audit, insurance, corporate administration, legal claims and regulatory compliance | Legal obligations; legitimate interests in operating and protecting our business and enforcing legal rights |
| Recruit and manage personnel and contractors | Steps before entering a contract; performance of a contract; legal obligations; legitimate interests in workforce management |

Where Attekus acts only as a processor of Customer Data, we process that data for the customer's documented purposes and instructions, not for an independent purpose except as permitted by the customer contract and applicable law.

## Sensitive information and children's information

We do not ordinarily seek sensitive information, special category data or criminal-offence data for our direct corporate activities. We may process such information where it is reasonably necessary for a permitted purpose and the requirements of applicable law are met, or where a customer configures a service to collect it and Attekus processes it on the customer's documented instructions. Where UK law applies, we will identify both an Article 6 lawful basis and an applicable Article 9 condition or lawful authority under Article 10. Where Australian or New Zealand law requires consent, we will obtain it unless another legal basis or exception applies.

Our corporate website and direct business activities are not directed to children. Customer-controlled portals may be used for activities involving children. In those circumstances the customer determines the collection and should provide the appropriate notice and obtain any required parent or guardian authorisation.

## Disclosure of personal information

We may disclose personal information, where lawful and reasonably necessary, to:

- Related Attekus entities: for group administration, support, service delivery and security;
- Attekus customers: where you use a customer-branded portal or service and the customer is responsible for your booking, registration, appointment, payment or other interaction;
- Service providers and subprocessors: including hosting, security, identity, communications, customer support, analytics, CRM, professional-services and payment providers;
- Integration and business partners: where an authorised integration or joint service requires information exchange. Appropriate contractual and security protections must be in place before the exchange begins;
- Professional advisers and insurers: including legal, accounting, audit, risk and insurance advisers;
- Government bodies, regulators, courts and law-enforcement agencies: where required or authorised by law or reasonably necessary to protect rights, safety or security;
- Transaction counterparties: in connection with a proposed or completed merger, financing, restructure, acquisition or sale, subject to confidentiality and legal safeguards; and
- Other recipients: with your consent or as otherwise permitted or required by law.

Attekus does not sell personal information.

## Overseas recipients and international transfers

Attekus may disclose personal information to overseas recipients depending on where the information originates, the relevant service and the customer's configuration, recipients may include related Attekus entities, customers and service providers located in Australia, New Zealand and the United Kingdom.

| Information originates in | Likely overseas recipient countries or regions |
|---|---|
| **Australia** | Australia, New Zealand |
| **New Zealand** | Australia, New Zealand |
| **United Kingdom** | Australia, New Zealand |

The hosting and support locations for Customer Data may be specified in the applicable customer contract, data-processing terms or service configuration. A

transfer may also occur through authorised remote access by support or security personnel as specified in the applicable customer contract.

Before making a cross-border disclosure, Attekus takes the steps required by applicable law. These may include reasonable steps and contractual measures under Australian Privacy Principle 8; checks and binding safeguards under New Zealand IPP 12; and, under UK law, reliance on adequacy regulations or appropriate safeguards such as the UK International Data Transfer Agreement or the UK Addendum, together with transfer risk assessments and supplementary technical or organisational measures where required.

We will update this policy or provide a service-specific collection notice if our likely disclosure practices materially change. You may contact the Privacy Officer for further information about the countries or transfer safeguard relevant to your information, or to request a copy or summary of the applicable safeguard, subject to legal, confidentiality and security restrictions.

## Cookies, analytics and direct marketing

Our website and services may use cookies and similar technologies that are essential for operation, remember preferences, maintain security, understand service use and improve performance. Where law requires consent for a non-essential technology, we will request it before use. You can use any cookie controls we provide and your browser settings, although disabling essential technologies may affect functionality.

We may send relevant service updates and, where permitted, marketing or event communications in accordance with applicable direct-marketing and electronic-communications laws. You can opt out of marketing at any time using the unsubscribe mechanism or by contacting us. Service and security communications may still be sent where necessary.

## Security and personal data breaches

We use reasonable technical and organisational measures designed to protect personal information from loss, misuse, interference, unauthorised access, modification and disclosure. Measures may include access controls, authentication, encryption where appropriate, logging and monitoring, secure development and change practices, personnel controls, supplier due diligence, backup and incident-response processes.

No transmission or storage system is completely secure. If a personal data breach occurs, we will assess it, take containment and remediation steps, and notify affected individuals, customers and regulators where required by applicable law.

## Retention

We retain personal information only for as long as reasonably necessary for the purpose for which it was collected, including to provide services, maintain security, resolve complaints, enforce contracts and meet legal, tax, accounting, audit, insurance and regulatory requirements. Retention periods are determined by the type and sensitivity of the information, the service and contractual requirements, legal limitation periods, security needs and the risk of harm from continued retention.

Customer Data is retained and deleted in accordance with the customer contract and documented instructions. When information is no longer required, we take reasonable steps to delete, destroy or de-identify it, subject to lawful retention requirements and secure backup cycles.

## Your privacy rights

Depending on the applicable law, the circumstances and whether Attekus is acting as a controller or processor of your personal information, you may have some or all of the following rights. This section provides a general summary only. These rights may be subject to conditions and exceptions under applicable law.

| Jurisdiction | Rights that may apply |
|---|---|
| Australia | Request access to, or correction of, personal information we hold about you; opt out of direct marketing; and complain to us about an alleged breach of the Australian Privacy Principles (APPs). Where lawful and practicable, you may also deal with us anonymously or using a pseudonym. |
| New Zealand | Request confirmation of whether we hold personal information about you and access to that information; request correction and, if the correction is not made, request that a statement of the correction sought be attached to the information; and complain to us and, if the matter is not resolved, to the New Zealand Privacy Commissioner about an alleged interference with your privacy, including a breach of the Information Privacy Principles (IPPs) under the Privacy Act 2020 (New Zealand). |

| Jurisdiction | Rights that may apply |
|---|---|
| United Kingdom | Request access, rectification, erasure, restriction or portability of your personal data; object to processing; withdraw consent where consent is the basis of processing, without affecting processing undertaken before withdrawal; and complain to the UK Information Commissioner's Office (ICO). The availability of these rights depends on the applicable lawful basis, the circumstances and any statutory exceptions. |

**Right to object - United Kingdom:** you have an absolute right to object to direct marketing at any time. You may also object to processing based on legitimate interests; we will stop unless we demonstrate compelling legitimate grounds or need the information for legal claims.

To exercise a privacy right, contact the Privacy Officer using the details below. We may request information reasonably necessary to verify your identity, authority and the scope of your request. We will respond within the period required by applicable law and will not charge a fee unless permitted by law.

A privacy right may be limited by applicable legal exceptions, the rights of others, legal privilege, security requirements or the capacity in which Attekus handles the relevant information.

If your request concerns Customer Data that Attekus processes on behalf of an Attekus customer, that customer will generally be responsible for responding to the request. You should contact the customer directly. Attekus may refer your request to the customer and assist the customer in responding.

## Automated decision-making

Attekus does not use personal information in its direct corporate dealings to make decisions based solely on automated processing that produce legal or similarly significant effects. If this changes, we will provide the information and safeguards required by law. A customer may configure or use data from the Attekus solution for its own decision-making; the customer's privacy notice governs that activity.

## Privacy complaints

You may complain about an actual or suspected breach of privacy by emailing info@attekus.com.au or writing to the Privacy Officer at the address below. Please use the subject line "Privacy complaint" and describe the conduct, the personal information involved and the outcome you are seeking. This information helps us

investigate, but we will not reject a complaint solely because it does not follow a particular form.

Attekus will:

- acknowledge the complaint promptly and, where UK law applies, no later than 30 days after receipt;
- make appropriate enquiries, assess the complaint fairly and keep you informed if additional time or information is required;
- respond without undue delay and ordinarily within 30 days, explaining the outcome and any action taken or proposed; and
- maintain an appropriate record of the complaint and use findings to improve our practices where appropriate.

If you are not satisfied, you may complain to the relevant regulator. Regulators may ask you to raise the matter with Attekus first and allow a reasonable period for response.

| Jurisdiction | Regulator | Information |
|---|---|---|
| Australia | Office of the Australian Information Commissioner (OAIC) | Complaint information |
| New Zealand | Office of the Privacy Commissioner | Complaint information |
| United Kingdom | Information Commissioner's Office (ICO) | Complaint information |

## Third-party links and services

Our website and services may link to third-party websites or services. Their privacy practices are governed by their own notices, and Attekus is not responsible for their independent handling of personal information.

## Changes to this policy

We may update this policy to reflect changes in law, technology, services or information-handling practices. We will publish the current version and effective date on our website and provide additional notice of material changes where required.

## Contact us

| Contact point | Details |
|---|---|
| Privacy contact | Attekus Privacy Officer |
| Email | info@attekus.com.au |
| Telephone | +61 2 8358 9160 |
| Australia | Attekus Pty Ltd, Level 1, Building 4, 40-52 McDougall Street, Milton, QLD, 4064, Australia. |
| New Zealand | Attekus NZ Limited, Suite 14376, 17B Farnham Street, Parnell, Auckland, 1052,<br>New Zealand. |
| United Kingdom | Attekus UK Limited, Swan Building, 20 Swan Street, Manchester, M4 5JW, United Kingdom. |

## Revision history

| Version | Revision date | Description of change | Author | Approved by | Approval date |
|---|---|---|---|---|---|
| 1 | 14/06/2023 | Created initial policy | Shane Bauskis | Peter Suchting | 14/06/2023 |
| 2 | 23/08/2023 | Added reference to the New Zealand Privacy Act 2020 | Shane Bauskis | Peter Suchting | 23/08/2023 |
| 3 | 26/07/2024 | Clarified payment handling and service-provider obligations | Konnor Ah kuoi | Peter Suchting | 26/07/2024 |
| 4 | 25/02/2026 | Added internal reference to Third Party Data Sharing Agreement template | Thomas Muller | Peter Suchting | 25/02/2026 |
| 5 | 30/07/2026 | Expanded for Australia, New Zealand and the United Kingdom; added complaints, overseas disclosures; updated outdated data-category references | Garth Kerr | Peter Suchting | 31/07/2026 |

Attekus

## About Attekus

Since 2017, Attekus has delivered booking, event and appointment solutions to public sector, education and commercial organisations across Australia and New Zealand. The Attekus Bookable application is used to support the delivery of community services across a wide range of operational environments, helping organisations manage complex bookings, events and appointments with confidence and control.

Attekus has been built around a deep understanding of service-driven environments where governance, accessibility, compliance and customer experience must work together. Our team brings extensive experience across local government, public sector and education sectors, and this knowledge is embedded into the design, configuration and ongoing evolution of the Attekus Bookable application. The result is a purpose-built solution that improves customer experience while also streamlining internal processes and operational efficiency.

**Experience starts here.**

attekus.com.au