POLICYCHECK

Privacy Policy

At PolicyCheck, we believe that data and technology play a vital part in innovation. We practice responsible data collection, which means considering the privacy, security and ethical implications of working with data, all the way from collecting it, to managing, using and deleting it.

We believe how we collect, process and store your data should be transparent and easy to understand. We have dedicated effort and resources to ensuring we adhere to best practices or better when it comes to the safety of your brand, your customers, privacy and security.

1. Introduction

PolicyCheck Ltd (NZBN:9429052521720) (“PolicyCheck”, “we”, “us”, “our”) is committed to protecting the privacy and security of consumers, our clients and brokers across Australia, New Zealand, and the United Kingdom. PolicyCheck complies with the New Zealand Privacy Act 2020 (the “NZ Act”), the Australian Privacy Act 1988 (the “AU Act”) including the Australian Privacy Principles (APPs) and guidance from the Office of the Australian Information Commissioner (OAIC), and, where applicable, UK data protection law including the UK GDPR and the Data Protection Act 2018 (the “UK Acts”).

This policy outlines how the PolicyCheck website, platform, or mobile application (collectively, the “Platform”) collect, use, store, and protect your personal information.

The Platform includes optional connections to third-party services (for example Google Drive) that you authorise so we can import documents you choose.

This policy does not limit or exclude any of your rights under the Act. If you wish to seek further information on the Act, see privacy.org.nz.

2. Key Definitions:

- “Broker” means a user who manages insurance policies and client data using the Platform.
- “Client” means an end-customer whose data is managed by a broker or who accesses the Platform directly.
- "Personal information" means any information about an identifiable individual, as defined under the New Zealand Privacy Act 2020 and the Australian Privacy Act 1988. This includes names, contact details, policy numbers, insurance history, and any other data that can be used to identify a person.
- “Platform” means the PolicyCheck website, web app, and mobile app.
- “LLM” means a large language model used for AI-enabled services (e.g., OpenAI Enterprise).
- “Connected Account” means a third-party account (such as a Google account) that you link to the Platform via OAuth or similar authorisation.
- “Integration Data” means metadata and content we access from a Connected Account solely as authorised by you (for example file names, folder paths, and document contents you select for import).

POLICYCHECK

Privacy Policy

3. Changes to this policy

We may change this policy by uploading a revised policy to this website. The change will apply from the date that we upload the revised policy.

4. Users of the Platform

PolicyCheck is designed for use by insurance brokers and their clients. As such, the Platform collects and processes information from:

- **Brokers:** Users who manage client data, submit insurance-related queries, and use the Platform to generate proposals and recommendations.
- **Clients:** End-customers who may log in to a client portal, submit personal or financial details, or review policy options.

We treat all data with the same high standards of confidentiality and security, regardless of whether it was provided directly by the client or indirectly by the broker on their behalf. Where brokers submit information about their clients, it is their responsibility to obtain the necessary consents to do so.

5. Sensitive Information

We will only collect 'sensitive information' with your consent. We collect information on the basis that you have obtained all necessary consents to share it with us, including any sensitive information. If this is not the case, please notify us at the time of providing the information.

6. Third Party (3rd Party) Information

You represent and warrant that you have obtained all necessary consents from that individual, and you agree to indemnify us against any claims arising from your failure to obtain such consent.

7. Personal Identifiable Information (PII)

We will take reasonable steps to keep your personal information safe from loss, unauthorised activity, or other misuse.

7.1. Consent for Personal Information Collection:

When collecting your personal information directly from you, we ensure that consent is clearly obtained, either through explicit consent forms or by providing clear and straightforward options to opt-in or opt-out where applicable.

7.2 Collection of Personal Information

We may collect personal information directly from you or someone you've authorised to deal with us on your behalf. This may happen through various interactions, such as:

- When you inquire about or seek a quote for a product or service.
- When you contact us by telephone, via mail, e-mail, or online.
- When you visit our website, including when you request a quote.
- When we supply any other products or services to you.
- When you participate in promotions, specials, or other offers with PolicyCheck.
- Obtaining your feedback on your customer experience.
- Conducting market research.
- Information that we indirectly obtain from you, such as information about the hardware and software you use accessing the PolicyCheck service, your IP address, the pages you access on the website, and other websites that you visit prior to accessing PolicyCheck.
- When you connect a third-party service (for example Google Drive): account identifiers needed to maintain the connection; OAuth access and refresh tokens; the scopes you approve; and Integration Data for files or folders you select to sync or import.
- We use cookies (an alphanumeric identifier that we transfer to your computer's hard drive so that we can recognise your browser) to monitor your use of the Platform. You may disable cookies by changing the settings on your browser, although this may mean that you cannot use all of the features of the website. Please refer to our Cookies Policy for more detail.
- For our general business operations (for example, maintenance of our business records, compliance with our legal and insurance obligations and statistical purposes.

Whenever we collect personal information from third parties, we ensure that these parties have lawful grounds to share this information with us, either through your direct consent or under the terms of their privacy policies.

7.3. Use of Personal Information

Your personal information is used for the following purposes:

- To verify your identity and authenticate you within our Platform
- To allow you to create an account
- To provide and improve our services, which may include using your data (and your clients data) to find relevant information on insurance products.
- To enhance website functionality and security, ensuring a secure and efficient user experience.
- To communicate with you about your inquiries or services you have engaged with, which may include sending updates or alerts related to your insurance preferences.
- To comply with legal and regulatory requirements, such as anti-fraud measures.

7.3.1 Impact on Individual Decisions:

The data we collect may be used to make decisions that directly affect the insurance options available to you. We commit to processing this information fairly and transparently, ensuring that all decisions are based on accurate and up-to-date information.

7.3.2 Data Anonymisation and Aggregation:

Where possible, we anonymise and aggregate personal information for analytical purposes. This process involves removing personally identifiable information to ensure that data cannot be linked back to any individual. By doing this, we aim to improve our services and develop better insights into consumer needs without compromising individual privacy.

7.4. Accessing, correcting or deleting your personal information

Subject to certain grounds for refusal set out in the Act, you have the right to access your readily retrievable personal information that we hold, to request a correction to your personal information, or request deletion of your personal data. Before you exercise this right, we will need evidence to confirm that you are the individual to whom the personal information relates.

In respect of a request for correction, if we think the correction is reasonable and we are reasonably able to change the personal information, we will make the correction. If we do not make the correction, we will take reasonable steps to note on the personal information that you requested the correction.

If you want to exercise any of the above rights, email us at support@policycheck.co.nz.

Your email should provide evidence of who you are and set out the details of your request (e.g. the personal information, the correction, or the request for deletion that you are requesting).

There may be circumstances which mean that information cannot be released to you. For example, these circumstances may include:

- the information may impact the privacy of another individual;
- the information is commercially sensitive evaluative information;
- the information is subject to solicitor-client or litigation privilege;
- PolicyCheck is prohibited by law from providing you with access; and
- the disclosure could be expected to threaten the safety, physical or mental health of an individual

If PolicyCheck decides that it cannot provide you with certain information, it will outline the reasons for its decision in writing and the mechanisms available to complain about the refusal.

7.5. Legal Basis for Processing Personal Information

We collect and process personal information based on one or more of the following legal grounds:

- Your consent;
- The necessity to perform a contract with you (or to take steps at your request before entering into a contract);
- Compliance with our legal obligations;
- Our legitimate interests, including providing and improving our services and ensuring security and fraud prevention, provided those interests are not overridden by your rights and interests.

POLICYCHECK

Privacy Policy

7.6 Connected third-party services (including Google Drive)

You may optionally connect Google Drive (or other providers we offer) so PolicyCheck can read documents or folders you select. We only request the access scopes shown on the provider's consent screen (for Google Drive this may include read-only Drive access). We do not use Connected Account access for advertising, selling personal information, or unrelated profiling. What we access: files and folders you choose to connect or sync; associated metadata (for example name, path, modified time); and credentials required to keep the connection working.

How we store credentials: OAuth tokens are encrypted at rest using industry-standard encryption (including cloud key management) and are accessible only to the Platform services that need them to perform the sync or import you requested.

What we do with Integration Data: we store imported documents in your tenant workspace and process them as part of PolicyCheck's insurance document and compliance features, subject to this policy and your organisation's instructions.

Disconnecting: you can disconnect Google (or other) integrations in Platform settings at any time. You may also revoke PolicyCheck's access in your Google Account security settings (Third-party access). After disconnection we stop new access; previously imported documents remain in your workspace until you or your organisation deletes them under our retention rules. Google's own processing of your Google Account is governed by Google's privacy policy. PolicyCheck's use of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

8. Retaining Your Information

At PolicyCheck, we are committed to only retaining information for as long as necessary to fulfil the purposes outlined in this Privacy Policy, unless a longer retention period is required by law or for auditing and regulatory purposes.

Here are our specific retention guidelines:

- **Client and Broker Information:** We retain personal, broker and client information for the duration of your relationship with us, plus a period of up to seven years after the relationship has ended. This period allows us to comply with legal and regulatory requirements and to resolve any disputes or claims.
- **Insurance Information:** Information related to insurance inquiries, policies, and transactions are retained for a minimum of seven years to comply with financial and insurance regulations in Australia and New Zealand.
- **Usage and Technical Information:** Data collected through cookies and other tracking technologies are generally retained for up to two years, after which they are anonymised or securely deleted. Please refer to our cookies policy.
- **Connected Account tokens:** retained only while the connection remains active, then securely deleted or invalidated within a reasonable period after you disconnect or revoke access (unless we must retain a limited audit record of the disconnection).
- **Integration Data / imported documents:** retained under the same Client and Broker / Insurance Information periods above, unless you delete them earlier.

- **Marketing Information:** If you opt out of receiving marketing communications from us, we will keep a record of your contact details and your decision to opt out to ensure that we do not contact you again for marketing purposes.

8.1 Destruction of Information:

When personal information is no longer needed, and we are not legally required to retain it, PolicyCheck ensures that such information is securely destroyed or de-identified.

8.2 Review and Update of Retention Policies:

Our data retention policies are regularly reviewed to ensure they remain compliant with current laws and regulations. Any changes to these policies will be communicated through updates to this Privacy Policy, ensuring transparency and compliance with data protection standards.

9. Use of Artificial Intelligence (AI)

PolicyCheck may use large language models (LLMs), including services provided by OpenAI Enterprise, to help process non-personal or de-identified insurance information and generate summaries or policy recommendations. These systems are used to enhance user experience and broker productivity.

Before sending data to these systems, we take reasonable steps to de-identify and anonymise personal information. However, we cannot guarantee that no personal data will ever be included in such submissions.

We have chosen OpenAI's Enterprise AI solution that does not retain data for training purposes and complies with our data protection standards. OpenAI's Enterprise service operates under strict confidentiality and data protection standards. Any data submitted is not used to train their models. Users should avoid entering unnecessary PII into free-text fields processed by AI.

9.1. AI-Related Risk Disclosures

While PolicyCheck undertakes best-practice measures to de-identify data prior to transmission to AI systems, users acknowledge that residual privacy risks may exist. In the event that any inadvertent disclosure of personal information to an AI processor occurs, we will assess the situation promptly and notify affected individuals where required by law.

10. DPA & Subprocessor Register

You can request a copy of our current subprocessor list or Data Processing Agreement (DPA) by contacting us at support@policycheck.co.nz.

11. Cross-Border Transfers

Some of our service providers are located outside New Zealand and Australia. Where we transfer personal information internationally, we ensure appropriate safeguards are in place, such as contractual clauses or reliance on trusted frameworks.

POLICYCHECK

Privacy Policy

For customers using policycheck.uk, we aim to process and store Platform data in the United Kingdom / EU region where our UK environment is hosted, subject to necessary transfers to subprocessors listed in our DPA / subprocessor register.

12. Internet use

The transfer of data over the Internet is inherently insecure. While we take reasonable steps to maintain secure internet connections, if you provide us with personal information over the internet, the provision of that information is at your own risk. i.e we cannot guarantee the security, during transmission, of any personal information provided to us via our website.

If you follow a link on our website to another site, the owner of that site will have its own privacy policy relating to your personal information. We suggest you review that site's privacy policy before you provide personal information.

13. Your Rights Under Privacy Laws:

PolicyCheck recognizes and supports your rights under the privacy laws of Australia and New Zealand. These rights include:

- **Access and Correction:** You have the right to access the personal information we hold about you and to request correction of any inaccurate, outdated, or incomplete information.
- **Data Portability:** Where applicable, you have the right to receive the personal data you have provided to us in a structured, commonly used, and machine-readable format, and the right to transmit that data to another controller without hindrance from us.
- **Right to Object:** You may object to the processing of your personal data based on your particular situation, especially in the case of profiling or direct marketing.
- **Right to be Informed of Breaches:** You have the right to be promptly informed in the event of a high-risk data breach that may affect your personal rights or freedoms.

Where UK law applies, you also have rights under the UK Acts (including access, rectification, erasure, restriction, objection, and portability, subject to exemptions).

13.1 Exercising Your Rights:

To exercise any of these rights, please contact us via the 'Contact Us' form. We will respond to your request within a reasonable timeframe and notify you of the action we have taken.

14. Privacy Complaints

Please contact us if you have any concerns or complaints about the manner in which we have collected or handled information. We will investigate your complaint and you can expect a response from us in writing within 30 days. If after our initial assessment of your complaint we decide that we need more information or that we'll need more time to respond to you, we'll let you know within a few days of receiving your complaint.

If you believe that we have not adequately addressed your concerns or have not complied with our obligations under the privacy laws, you have the right to lodge a complaint with the relevant

authority. In Australia, complaints can be directed to the Office of the Australian Information Commissioner (OAIC). In New Zealand, complaints should be addressed to the Office of the Privacy Commissioner (OPC).

- Australia: Contact the OAIC via their website at www.oaic.gov.au or call their hotline.
- New Zealand: Contact the OPC via their website at www.privacy.org.nz

In the United Kingdom, complaints can be directed to the Information Commissioner's Office (ICO) at www.ico.org.uk.

15. Direct Marketing Communications:

PolicyCheck utilises your personal information to inform you about products, services, and offers from PolicyCheck and our business partners that we believe may be of interest to you. You may receive marketing communications via mail, telephone, email, SMS, or social media.

15.1 Consent and Your Preferences:

We only send you direct marketing communications with your explicit consent, which we obtain at the point of data collection. When collecting your contact details, we provide clear options allowing you to opt-in or opt-out of receiving marketing materials. These options are designed to respect your choice and control over your personal information.

15.2 Managing Your Marketing Preferences

You can manage your marketing preferences at any time:

- **Via Your Account:** Log into your account on our website to adjust your marketing preferences.
- **Direct Communication:** You can opt out of receiving direct marketing by using the unsubscribe link provided in each marketing email, by replying STOP to SMS messages, or by following the opt-out instructions included in any other communication medium.

We ensure that opt-out requests are processed promptly and that you will not be included in future marketing communications once an opt-out has been registered.

15.3 Further Information and Complaints:

Should you have any questions about our direct marketing practices or if you feel that your preferences have not been adequately respected, please contact us via the 'Contact Us' form. You also have the right to lodge a complaint with the relevant privacy authority if you believe we have not adhered to marketing consent regulations.

16. Security Measures

We implement a range of administrative, technical, and physical safeguards designed to protect the personal information we hold. These include encryption, access controls, secure storage, regular audits, and staff training. While no system is completely secure, we take appropriate steps to reduce the risk of data breaches.

In the event of a notifiable data breach, we will notify affected individuals and the relevant authorities without undue delay, in accordance with our internal Data Breach Response Plan and applicable laws.

17. Contact Us

If you have any questions about this privacy policy, our privacy practices, or if you would like to request access to, or correction of, your personal information, you can contact us at support@policycheck.co.nz (or, for UK customers, the support address published on policycheck.uk).

This policy is effective as of May 2024.
Document version 1.16
Last updated on September 22nd 2026