POLICYCHECK

Document Processing Agreement

Introduction

This Document Processing Agreement (“Agreement”) describes how PolicyCheck processes documents and data uploaded to, or generated within, the PolicyCheck platform, products, services, and related tools (collectively, the “Services”). It also describes the security and privacy controls applied to protect that information.

By uploading documents to the Services or otherwise enabling document processing, you agree to this Agreement. If you do not agree, you must not upload documents or use document processing features.

This Agreement applies to all users of PolicyCheck, including brokers, advisers, firms, partners, and any authorised users acting on their behalf.

Purpose of PolicyCheck

PolicyCheck provides software tools designed to assist insurance brokers and advisers in reviewing, structuring, comparing, and managing insurance information.

PolicyCheck is:

- A technology platform and decision-support tool
- Not an insurer, underwriting agent, or adviser
- Not a provider of financial, insurance, or legal advice

All outputs generated by the platform are intended to support professional judgment, not replace it.

Definitions

For the purposes of this Agreement:

- Customer means the organisation or person using the Services.
- Customer Data means any data, documents, content, or information uploaded to the Services, or generated from that content (including extracted data, summaries, comparisons, and reports).
- Personal Information / PII means information that identifies, or could reasonably identify, an individual (including personal details contained in insurance documentation and communications).
- Processing means any operation performed on Customer Data, including ingestion, parsing, classification, extraction, transformation, indexing, summarisation, comparison, reporting, and storage.
- LLM means a large language model used to support features such as summarisation, extraction, comparison, drafting, or interpretation assistance.

POLICYCHECK

Document Processing Agreement

Scope of Processing

PolicyCheck may process Customer Data to provide Services including (without limitation):

- Uploading, storing, and organising insurance documents and packs
- Splitting documents into structured components (e.g., schedule, wording, endorsements, certificates, appendices)
- Extracting structured data (e.g., limits, deductibles, endorsements, exclusions, conditions, parties, dates)
- Identifying and flagging key terms, mismatches, or gaps against provided requirements or needs
- Comparing policy clauses and versions
- Generating summaries, tables, and client-ready outputs
- Producing compliance checks and audit evidence for workflows performed within the platform

Processing may be automated and may involve AI-assisted workflows, including LLMs, where enabled.

Use of LLMs and AI-Assisted Processing

Some features of the Services use LLMs or other automated techniques to process Customer Data and generate outputs.

You acknowledge that:

- AI-generated outputs may contain errors, omissions, or misinterpretations
- Outputs depend on the quality, completeness, and context of the documents and inputs provided
- PolicyCheck does not warrant that AI outputs are accurate, complete, or fit for a particular purpose
- Outputs must be reviewed by a qualified broker or adviser before use with clients, insurers, regulators, or any third party

PolicyCheck does not provide financial, insurance, or legal advice, and AI outputs must not be represented as advice, recommendations, or determinations of suitability.

PII Removal and Obfuscation Controls

PolicyCheck is designed to reduce exposure of Personal Information within AI processing where feasible and appropriate for the workflow.

Unless a feature explicitly requires identifiable information to function (e.g., producing a client-addressed document), PolicyCheck applies controls intended to:

- Detect Personal Information in uploaded documents and extracted text
- Obfuscate or redact Personal Information before sending relevant text to LLM-based processing where feasible

- Minimise the amount of Personal Information used in prompts and AI context windows
- Prevent unnecessary Personal Information from being included in AI-generated outputs

You acknowledge that:

- Documents you upload may contain Personal Information, and you are responsible for ensuring you have the right to upload and process that information
- No automated redaction process is perfect; residual Personal Information may remain in some cases (e.g., complex formatting, scanned documents, embedded images, handwritten notes)
- PolicyCheck may provide configuration options or workflow patterns to further reduce Personal Information exposure (for example, “PII-safe mode” workflows or policy templates that avoid personal identifiers)

Storage and Security of Customer Data

PolicyCheck stores Customer Data using industry-standard cloud infrastructure and security practices.

Data Storage Locations

Customer Data may be stored within services including:

- Amazon Web Services (AWS), including Amazon S3 for file/object storage
- AWS-managed relational databases (RDS) for structured application and audit data
- MongoDB Atlas for document-oriented data storage where used by the platform

PolicyCheck may use additional supporting services for logging, monitoring, and operational security consistent with the delivery of the Services.

Security Controls (At Rest and In Transit)

PolicyCheck applies controls intended to protect Customer Data, including:

- Encryption in transit using TLS (or equivalent secure transport)
- Encryption at rest for stored data (including object storage and databases), using provider-supported encryption mechanisms
- Access controls designed to enforce least-privilege and restrict access to authorised users and systems
- Logical separation controls intended to reduce risk of unauthorised cross-customer access
- Monitoring and logging mechanisms to support detection and investigation of suspicious activity

Access and Operational Controls

PolicyCheck may implement and maintain:

- Role-based access controls and environment separation (e.g., production vs staging)
- Administrative safeguards including change controls and credential management
- Audit logs for key platform and processing actions (where enabled within the Services)

POLICYCHECK

Document Processing Agreement

Data Retention and Deletion

PolicyCheck retains Customer Data for as long as required to provide the Services, meet contractual commitments, and support legitimate operational and compliance needs.

Where supported by the platform or contract:

- You may request deletion of Customer Data, subject to legal retention obligations and technical constraints (e.g., backups and disaster recovery copies)
- PolicyCheck may retain de-identified or aggregated operational metrics that do not identify customers or individuals

Retention periods may vary based on the Services used, configuration, and applicable legal or regulatory obligations.

Confidentiality

PolicyCheck will treat Customer Data as confidential and will implement reasonable safeguards to protect it from unauthorised access, disclosure, or misuse.

You agree to keep your access credentials confidential and to ensure your authorised users follow appropriate internal security and confidentiality practices.

Customer Responsibilities

You are responsible for:

- Ensuring you have lawful authority to upload and process documents and Personal Information
- Ensuring your use of the Services complies with privacy, confidentiality, record-keeping, and regulatory obligations
- Reviewing all outputs (including AI-generated outputs) before relying on them
- Ensuring users do not upload malicious content or attempt to compromise the Services
- Using the Services only for professional and lawful purposes within your authorised scope

Prohibited Use Related to Data and AI

You must not:

- Use the Services to process unlawful content or content that you do not have rights to use
- Attempt to reverse-engineer, extract, or replicate PolicyCheck models, prompts, workflows, or system logic
- Use the Services to train competing AI systems or to build datasets for competitive model training
- Circumvent access controls, audit mechanisms, PII safeguards, or security protections
- Upload content intended to test, evade, or disable redaction/obfuscation, security, or monitoring controls

POLICYCHECK

Document Processing Agreement

Early-Stage Platform Notice

PolicyCheck is an evolving platform and may be in active development.

You acknowledge that:

- Features may change, improve, or be withdrawn
- AI outputs may vary over time as models and logic evolve
- Some controls (including redaction and automation) may be improved iteratively and may not cover all edge cases

If you are unsure about platform behaviour or appropriate handling of sensitive data, you should contact PolicyCheck before relying on a workflow.

Limitation of Liability

To the maximum extent permitted by law:

- Use of the Services is at your own risk
- PolicyCheck disclaims liability arising from reliance on outputs, including AI-generated outputs
- PolicyCheck is not responsible for client outcomes, claims disputes, underwriting decisions, or regulatory action arising from your use of the Services

Nothing in this Agreement limits liability where such limitation is prohibited by law.

Changes to This Agreement

We may update this Document Processing Agreement from time to time to reflect changes in the platform, legal requirements, security practices, or operational processes.

Updates will be published with a revised version and effective date

Contact Us

If you have questions about this Policy or appropriate use of the Services, please contact the PolicyCheck team via our official support channels.

This policy is effective as of May 2024.
Document version 1.13
Last updated on Feb 18th 2026