

EXTRACT BY DOCOMPAREAI / LEGAL

Extract by DocompareAI Privacy Policy

How Extract by DocompareAI collects, uses and protects personal information

EFFECTIVE DATE 25 August 2026
OPERATOR OZKAI (ABN 44 606 005 308)
CONTACT contact@docompareai.com

This Privacy Policy explains how Extract by DocompareAI handles personal information when you use <https://extract.docompareai.com> and its related PDF extraction, trial, subscription and support services (the **Service**). The Service is operated by OZKAI (ABN 44 606 005 308). Extract and DocompareAI are product and brand names used by OZKAI and are not separate legal entities. In this policy, **OZKAI**, **we**, **us** and **our** mean the operator of the Service.

We handle personal information in line with this policy and, where applicable, the Privacy Act 1988 (Cth). This policy applies to account holders, trial users, paid users, people who contact us and people whose information is included in material submitted to the Service.

1. Information we collect

We collect account and identity information such as your email address, display name, sign-in provider and account identifiers. If you use Google sign-in, Google provides the identity information needed to create or access your account.

We collect service information such as uploaded PDFs, extracted text, field definitions, instructions, templates, generated results, source references, usage records and deletion status. We also collect messages, feedback and attachments you send when requesting support.

We collect billing and subscription information such as your plan, Stripe customer and subscription identifiers, payment status, billing dates and limited transaction information. Stripe collects and processes complete payment card details. We do not receive or store complete card numbers or card security codes.

We may collect technical information such as IP address, browser and device information, session and authentication records, timestamps, request identifiers, error details, security events and information about how features are used.

2. How we use information

We use information to create and secure accounts; provide PDF extraction and review features; manage trials, subscriptions, quotas and payments; communicate about the Service; provide support; investigate errors, fraud, abuse and security incidents; maintain and improve the Service; comply with law; and protect our rights and the rights of users and others.

We send essential account, billing, security and service messages when needed. We will only send marketing messages where permitted by law. You can unsubscribe from marketing without stopping essential service messages.

We do not sell personal information.

3. PDF and AI processing

The Service processes uploaded PDFs on its servers. Depending on the current configuration and the feature used, it may send a complete PDF, extracted text, document snippets, field definitions and instructions to Google Gemini, OpenAI or both. A different provider may be used for instruction generation and extraction.

AI providers process submitted material to return generated instructions or extraction results. Their handling of data is also governed by our account arrangements with them and their applicable service terms. We do not promise that a particular provider, model, processing country or retention setting will always apply.

AI output and diagnostic records may include personal information from an uploaded document. Do not upload information that the Terms of Service prohibit. You are responsible for having a lawful basis and any required authority or consent to submit information about another person.

4. Service providers and disclosure

We disclose information to providers that help operate the Service. These may include Supabase for authentication and application data, Vercel for web hosting, Render for processing services, Stripe for billing, storage and database providers, and Google or OpenAI for AI processing. If enabled, PostHog may provide product analytics and Sentry may provide error monitoring.

We may also disclose information to professional advisers, insurers, regulators, law enforcement or courts where reasonably necessary or required by law. If the Service or its assets are involved in a genuine sale, financing or reorganisation, relevant information may be disclosed under appropriate confidentiality arrangements.

We do not allow providers to use personal information for unrelated purposes on our behalf. Providers may, however, have their own independent obligations and permitted uses under their terms and applicable law.

5. Overseas processing

Extract uses cloud and AI providers that may process or store information outside Australia, including in the United States and other countries where those providers or their subprocessors operate. Privacy protections in those countries may differ from Australian law.

We take reasonable steps, where required, when engaging providers and handling overseas disclosures. We do not offer a guaranteed Australian data residency option. If your organisation cannot permit overseas cloud or AI processing, do not upload the information.

6. Retention and deletion

Jobs currently have a default retention period of seven days from creation. Automated cleanup removes eligible records and queues stored objects for deletion. Active or queued jobs, provider delays, retries, backups and technical problems may postpone final deletion.

You can delete a job or request account deletion through available controls. Authentication deletion may be retried if a provider is unavailable, and a limited deletion record may be kept temporarily to complete the process. You should download any output you need before deletion or expiry because we may not be able to restore it.

We retain account, support, billing, transaction, usage and security records only for as long as reasonably needed to provide the Service, meet legal and accounting obligations, resolve disputes, prevent fraud and protect the Service. Stripe and other providers retain information under their own policies. Backup copies may remain for a limited period before being overwritten.

Deleting an Extract account does not itself cancel an active Stripe trial or subscription. Cancel through the Stripe billing portal before deleting the account if you want billing to stop.

7. Cookies and browser storage

The Service may use cookies and browser local storage to keep you signed in, protect sessions, remember choices and support essential functions. Authentication access and refresh tokens may be stored in browser local storage. Anyone with access to an unlocked browser profile may be able to use the session, so sign out on shared or untrusted devices.

If analytics or error monitoring is enabled, those tools may use cookies or similar technologies and collect device, usage and error information. Where required, we will provide notice or seek consent. Browser controls can block or delete storage, but this may prevent account and extraction features from working correctly.

8. Security

We use reasonable technical and organisational measures intended to protect information, including authentication, access controls, encrypted network connections and provider security controls. Access is limited to people and systems that need it to operate, secure or support the Service.

No online service is completely secure. We cannot guarantee that information will never be lost, misused or accessed without authorisation. Use a secure device and email account, protect your sign-in session and tell us promptly if you suspect a security problem.

9. Restricted information and children

Extract is not designed for patient records, identifiable health information, genetic or biometric information, government identity documents, financial credentials, children's data, legally privileged documents or other regulated or highly sensitive material. The full restrictions are in the Terms of Service. Do not upload that information, even if you have consent, unless we have expressly agreed in writing to appropriate arrangements.

The Service is for users aged 18 or older and is not directed to children. If you believe a child has created an account or that children's information has been uploaded, contact us so we can investigate and delete it where appropriate.

10. Access, correction and complaints

You may ask to access or correct personal information we hold about you, or make a privacy complaint, by emailing contact@docompareai.com. We may need to verify your identity before responding. We may refuse or limit a request where permitted by law, including where disclosure would affect another person's privacy or reveal protected information.

We will acknowledge and investigate privacy complaints within a reasonable time. If you are not satisfied and Australian privacy law applies, you may be able to complain to the Office of the Australian Information Commissioner at <https://www.oaic.gov.au>.

11. Your choices

You can choose not to provide optional information, but some information is necessary to create an account, process documents or manage payment. You can stop uploading documents, delete eligible jobs, cancel a subscription and request account deletion. Cancellation and deletion are separate actions.

You can unsubscribe from marketing messages using the link in the message or by contacting us. Essential account, transaction, billing and security messages may still be sent while relevant.

12. Changes and contact

We may update this policy as the Service, providers or legal requirements change. We will publish the updated version and effective date. If a change materially affects how we use information already collected, we will provide any additional notice or choice required by law.

For privacy questions, requests or complaints, contact:

OZKAI

ABN 44 606 005 308

NSW 2147, Australia

contact@docompareai.com