

LIVING OFF AI

BENUTZERHANDBUCH

REDACT FOR AI

Pseudonymisieren Sie juristische Dokumente auf Ihrem Computer. Arbeiten Sie mit KI, ohne Mandantendaten preiszugeben.

WAS DIE SOFTWARE TUT

Mandantendaten verlassen diesen Computer nie.

Redact for AI läuft vollständig auf Ihrem Rechner. Die Software findet in einem juristischen Dokument die personenbezogenen Daten (Namen, Unternehmen, Kennnummern, Anschriften, Bankverbindungen) und ersetzt jede durch einen gleichbleibenden Platzhalter (**Persona_1, Client_1...**).

Sie prüfen das Ergebnis, schicken den pseudonymisierten Text an die KI und stellen die echten Namen in deren Antwort mit einem Klick wieder her. Keine Cloud, kein Server, kein Netz: die Software arbeitet auch ohne Verbindung.

01 Originaldokument	02 Pseudonymisierte Kopie	03 Die KI arbeitet mit Platzhaltern	04 Echte Namen wiederhergestellt
-------------------------------	-------------------------------------	---	--

DIE DREI REGELN

▲ Nur der pseudonymisierte Text geht an die KI.

Das Original verlässt seinen Ordner nie. Was Sie aus der App kopieren, enthält Platzhalter, keine Daten.

▲ Prüfen Sie jedes Dokument.

Automatische Erkennung ist nie hundertprozentig. Kontrollieren Sie die Vorschau, vor allem das, was nicht markiert ist, bevor Sie kopieren.

▲ Teilen Sie den Ordner `_private` nie.

Er enthält die Zuordnungen von Platzhaltern zu echten Namen. Er bleibt auf diesem Computer.

INSTALLATION

Zehn Minuten, einmalig.

macOS

- 01 Entpacken und **Redact for AI.app** an einen beliebigen Ort verschieben.
- 02 Erster Start: macOS blockiert nicht signierte Apps. Öffnen Sie Systemeinstellungen, Datenschutz und Sicherheit, scrollen Sie zum Hinweis und wählen Sie Trotzdem öffnen. Nur einmal.
- 03 Der erste Start lädt die Sprachmodelle: 30 bis 60 Sekunden.

Windows

- 01 Ordner entpacken und **RedactForAI.exe** öffnen.
- 02 Erscheint SmartScreen, wählen Sie Weitere Informationen und dann Trotzdem ausführen. Nur einmal.
- 03 Der erste Start lädt die Sprachmodelle: 30 bis 60 Sekunden.

Die Sprache der Oberfläche (English, Italiano, Português, Español, Français, Deutsch) finden Sie im Menü oben rechts. Beim ersten Start fragt die App, in welchen Sprachen Sie arbeiten, und lädt für jede das Paket der erweiterten Erkennung herunter.

TÄGLICHER GEBRAUCH

Pseudonymisieren und prüfen.

- 01 Wählen Sie die Datei (PDF, Word, Text oder Scan, die Texterkennung startet von selbst) und die Sprache des Dokuments.
- 02 Drücken Sie Pseudonymisieren. Alles Erkannte wird in der Vorschau gelb markiert.
- 03 Ergänzen Sie, was die Software übersehen hat: Text markieren und Hinzufügen drücken. Klicken Sie eine Markierung an, um einen Fehltreffer zu entfernen oder eine Rolle zuzuweisen (Mandant, Gegenpartei, Zeuge). Rollen machen den pseudonymisierten Text für die KI lesbar.
- 04 Haken Sie Ich habe die Vorschau geprüft an, drücken Sie Pseudonymisierten Text kopieren und fügen Sie ihn in die KI ein.
- 05 Ist das Original eine Word-Datei, exportiert Als Word speichern eine pseudonymisierte .docx mit erhaltener Formatierung.

DIE NAMEN ZURÜCKHOLEN

Echte Namen wiederherstellen.

- 01 Öffnen Sie den zweiten Tab, Echte Namen wiederherstellen.
- 02 Fügen Sie den KI-Entwurf ein, samt Platzhaltern.
- 03 Drücken Sie Wiederherstellen und wählen Sie den Speicherort. Die gespeicherte Datei enthält echte Daten: sie geht nie an eine KI.

KANZLEI-EINSTELLUNGEN

Zwei Listen, neben der App.

termini_riservati.txt: Begriffe, die immer pseudonymisiert werden, der Name der Kanzlei, wiederkehrende Mandanten, alles was die Erkennung nie übersehen darf. Ein Begriff pro Zeile.

termini_sicuri.txt: Begriffe, die nie gemeldet werden. Nützlich für Plattformnamen oder Vokabular, das die Software fälschlich markiert.

DIE GRENZEN KENNEN

- ▲ Datumsangaben bleiben bewusst lesbar: juristische Dokumente brauchen sie.
- ▲ Eine Beschreibung kann eine Person identifizieren, ohne sie zu nennen. Die Prüfung deckt ab, was Software nicht sehen kann.
- ▲ Gescannte PDFs brauchen die richtige Dokumentsprache für die Texterkennung.
- ▲ Lassen Sie die Festplattenverschlüsselung aktiv: FileVault unter macOS, BitLocker unter Windows.