Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO für Immorento

Stand: 16. November 2026

Dieser Auftragsverarbeitungsvertrag („AVV“) konkretisiert die Verarbeitung personenbezogener Daten durch die digitally induced GmbH im Auftrag des Kunden bei Nutzung von Immorento, insbesondere der Daten seiner Mieter und anderer Dritter. Er gilt zusammen mit der Nutzungsvereinbarung und einer etwaigen Bestellung oder Individualvereinbarung als Hauptvertrag.

Parteien

Dieser AVV wird geschlossen zwischen dem Kunden, der Immorento als Vermieter oder Eigentümer im eigenen Namen oder im Namen einer Organisation nutzt (nachfolgend „Auftraggeber“ oder „Verantwortlicher“), und

digitally induced GmbH
Schanzenstraße 96
40549 Düsseldorf
Deutschland

als Auftragsverarbeiter (nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“). Auftraggeber und Auftragnehmer werden gemeinsam die „Parteien“ genannt.

Für die Daten seiner Mieter und anderer Dritter ist der Auftraggeber Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, auch wenn er als Verbraucher privat vermietet.

1. Gegenstand und Rangfolge

1. Der Auftragnehmer stellt dem Auftraggeber die Software Immorento bereit, einen Assistenten für die Verwaltung vermieteter Wohnungen und Häuser. Der Dienst nimmt Dokumente zu den Objekten des Auftraggebers über Telegram, die Weboberfläche, die iOS-App, E-Mail-Weiterleitung, verbundene Postfächer, Cloud-Speicher und Online-Portale entgegen und legt sie nach Objekt, Einheit und Mietverhältnis ab. Er gleicht Bankumsätze mit Mietverhältnissen ab, sucht Rechnungen zu Ausgaben, bereitet Nebenkostenabrechnungen, Anlage-V-Übersichten, Schreiben an Mieter und Überweisungen als Entwürfe vor, versendet vom Auftraggeber freigegebene Schreiben und erinnert an Fristen.
2. Soweit der Auftragnehmer dabei personenbezogene Daten verarbeitet, für die der Auftraggeber Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist, erfolgt diese Verarbeitung ausschließlich im Auftrag und nach Weisung des Auftraggebers nach Maßgabe dieses AVV.
3. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV für datenschutzrechtliche Fragen der Auftragsverarbeitung vor.

2. Art, Zweck und Dauer der Verarbeitung

1. Art, Zweck, Umfang, Kategorien personenbezogener Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.
2. Die Verarbeitung dient der vertragsgemäßen Bereitstellung von Immorento, insbesondere der Ablage und Auswertung von Dokumenten zu den Objekten, dem Abgleich von Zahlungen mit Mietverhältnissen, der Vorbereitung von Nebenkostenabrechnungen, Schreiben und Überweisungen sowie dem Versand von Schreiben nach Freigabe durch den Auftraggeber.
3. Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Nach Ende des Hauptvertrags werden Auftraggeber-Daten nach Ziffer 11 gelöscht oder herausgegeben, soweit keine gesetzlichen Aufbewahrungspflichten oder berechtigten Nachweiszwecke entgegenstehen.

3. Weisungen des Auftraggebers

1. Die Weisungen des Auftraggebers ergeben sich anfänglich aus diesem AVV, dem Hauptvertrag, den Einstellungen im Produkt, verbundenen Integrationen sowie den vom Auftraggeber oder seinen Nutzern erteilten Anweisungen über Weboberfläche, iOS-App, Telegram, E-Mail oder einen vom Auftraggeber verbundenen KI-Assistenten.
2. Gibt der Auftraggeber ein Schreiben frei, weist er den Auftragnehmer damit an, es an den genannten Empfänger zu übermitteln, bei Briefen über den in Anlage 2 genannten Druck- und Versanddienstleister.
3. Einzelweisungen können in Textform erteilt werden. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungs- oder Vertragsänderung behandelt.
4. Der Auftragnehmer verarbeitet Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht nach Unionsrecht oder deutschem Recht zu einer anderen Verarbeitung verpflichtet ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber vorab, soweit das betreffende Recht dies nicht untersagt.
5. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist er den Auftraggeber darauf hin und darf die Durchführung der Weisung bis zur Bestätigung oder Änderung aussetzen.

4. Verantwortung des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Rechtmäßigkeit der Übermittlung an den Auftragnehmer, die Richtigkeit der bereitgestellten Daten und die Wahrung der Rechte betroffener Personen verantwortlich.
2. Der Auftraggeber informiert seine Mieter und andere betroffene Personen über die Verarbeitung, soweit er dazu nach Art. 13 und 14 DSGVO verpflichtet ist.
3. Der Auftraggeber stellt sicher, dass nur berechtigte Nutzer Zugriff auf sein Konto, seine Organisation, verbundene Postfächer, Bankzugänge, Portale und seinen Telegram-Chat mit dem Dienst erhalten.
4. Der Auftraggeber prüft Entwürfe, insbesondere Nebenkostenabrechnungen, Mieterhöhungen und Schreiben an Mieter, sowie sonstige KI-Ausgaben vor ihrer Verwendung. Immorento erbringt keine Rechts- oder Steuerberatung.

5. Vertraulichkeit und Personal

1. Der Auftragnehmer verpflichtet alle Personen, die Auftraggeber-Daten verarbeiten können, zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Der Zugriff auf Auftraggeber-Daten wird auf Personen beschränkt, die ihn zur Leistungserbringung, Wartung, Sicherheit, Support oder Fehleranalyse benötigen.

6. Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die zum Stand dieses AVV getroffenen Maßnahmen sind in Anlage 3 beschrieben.
2. Der Auftragnehmer darf technische und organisatorische Maßnahmen weiterentwickeln und ersetzen, sofern das vertraglich vereinbarte Schutzniveau nicht wesentlich unterschritten wird.
3. Auftraggeber-Daten werden nicht zum Training eigener oder fremder KI-Modelle verwendet. Soweit KI-Modell-Anbieter eingesetzt werden, erfolgt dies im Rahmen der in Anlage 2 beschriebenen Unterauftragsverarbeitung und Transfermechanismen.

7. Weitere Auftragsverarbeiter

1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Die bei Vertragsschluss genehmigten weiteren Auftragsverarbeiter sind in Anlage 2 aufgeführt.
2. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen durch Hinzufügung oder Ersetzung weiterer Auftragsverarbeiter über die Trust-Seite, per E-Mail oder auf anderem geeigneten Weg. Der Auftraggeber kann aus wichtigem Grund innerhalb von 14 Tagen nach Information widersprechen.
3. Erhebt der Auftraggeber einen begründeten Widerspruch und ist dem Auftragnehmer die Leistungserbringung ohne den betroffenen weiteren Auftragsverarbeiter nicht zumutbar, kann jede Partei den Hauptvertrag und diesen AVV mit einer Frist von 30 Tagen kündigen.
4. Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten dieses AVV im Wesentlichen entsprechen.

8. Drittlandübermittlungen

1. Eine Verarbeitung findet grundsätzlich innerhalb der EU oder des EWR statt. Einzelne weitere Auftragsverarbeiter können Daten in Drittländern verarbeiten, insbesondere in den USA.
2. Drittlandübermittlungen erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch Angemessenheitsbeschluss, EU-Standardvertragsklauseln, das EU-US Data Privacy Framework oder einen anderen zulässigen Transfermechanismus.

9. Unterstützungspflichten

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren durch geeignete technische und organisatorische Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO. Wendet sich ein Mieter oder eine andere betroffene Person mit einem solchen Antrag unmittelbar an den Auftragnehmer, leitet er den Antrag an den Auftraggeber weiter.
2. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden.
3. Soweit der Auftragnehmer durch Unterstützungsleistungen einen Aufwand hat, der über die übliche Leistungserbringung hinausgeht, kann er eine angemessene Vergütung verlangen, sofern gesetzlich nichts anderes zwingend vorgeschrieben ist.

10. Datenschutzverletzungen

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Auftraggeber-Daten bekannt wird.
2. Die Information enthält, soweit verfügbar, die Art der Verletzung, betroffene Daten- und Personenkategorien, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Abmilderung.
3. Der Auftragnehmer trifft unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

11. Löschung und Herausgabe

1. Nach Abschluss der Verarbeitungsleistungen löscht der Auftragnehmer Auftraggeber-Daten oder gibt sie heraus, soweit der Auftraggeber dies verlangt und keine gesetzlichen Aufbewahrungspflichten oder berechtigten

Nachweiszwecke entgegenstehen.

2. Einzelne Dokumente, Mietverhältnisse und Verbindungen kann der Auftraggeber selbst löschen oder trennen. Vor einer Kontolöschung kann er seine Dokumente exportieren. Fordert er die Löschung seines Kontos an, beginnt sie nach einer Wartefrist von fünf Tagen, in der er sie zurückziehen kann; Sicherungskopien werden im vorgesehenen Löschzyklus überschrieben. Aufbewahrungspflichten des Auftraggebers als Vermieter bleiben unberührt.
3. Dokumentationen, Protokolle und Nachweise, die der Auftragnehmer zur Erfüllung rechtlicher Pflichten, zur Sicherheit, zur Abrechnung oder zur Verteidigung gegen Ansprüche benötigt, dürfen nach Vertragsende aufbewahrt werden, soweit erforderlich.

12. Nachweise und Überprüfungen

1. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem AVV zur Verfügung.
2. Der Auftraggeber ist berechtigt, die Einhaltung dieses AVV zu überprüfen. Inspektionen vor Ort bedürfen einer angemessenen Vorankündigung, dürfen den Betriebsablauf nicht unverhältnismäßig stören und sind auf die für den Nachweis erforderlichen Informationen beschränkt.
3. Der Auftragnehmer darf vertrauliche Informationen, Informationen zu anderen Kunden, Geschäftsgeheimnisse und sicherheitskritische Details schützen oder nur in angemessen geschwärzter Form bereitstellen.
4. Der Auftragnehmer kann den Nachweis auch durch geeignete Dokumentationen, Zertifizierungen, Sicherheitskonzepte, Prüfberichte oder gleichwertige Nachweise erbringen.

13. Haftung

Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags. Zwingende gesetzliche Ansprüche nach Datenschutzrecht bleiben unberührt.

14. Laufzeit und Schlussbestimmungen

1. Dieser AVV gilt ab Annahme der Nutzungsvereinbarung oder ab sonstigem Abschluss des Hauptvertrags und endet mit dem Hauptvertrag, soweit sich aus diesem AVV oder gesetzlichen Pflichten nichts Abweichendes ergibt.
2. Änderungen dieses AVV bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist.
3. Es gilt deutsches Recht. Ausschließlicher Gerichtsstand für Kaufleute ist, soweit zulässig, Düsseldorf.

Ort, Datum	Ort, Datum
Auftraggeber	digitally induced GmbH

Anlage 1: Verarbeitungstätigkeiten

Gegenstand	Bereitstellung von Immorento als SaaS-Assistent für Vermieter: Ablage von Dokumenten nach Objekt, Einheit und Mietverhältnis, Abgleich von Mieteingängen, Rechnungen zu Ausgaben, Nebenkostenabrechnungen, Anlage-V-Übersichten, Schreiben an Mieter und Erinnerungen an Fristen.
Zwecke	Betrieb des Kontos, Authentifizierung, Support, Abruf von Bankumsätzen und ihr Abgleich mit Mietverhältnissen, Prüfung neuer E-Mails in verbundenen Postfächern, Abruf von Dokumenten aus Cloud-Speichern und Online-Portalen, Verarbeitung hochgeladener Dokumente, KI-gestütztes Auslesen, Klassifizieren und Zuordnen, Telegram-Kommunikation, Entwürfe von Nebenkostenabrechnungen, Anlage-V-Übersichten, Schreiben an Mieter und Überweisungen, Druck und Versand freigegebener Briefe, Erinnerungen an Fristen.
Art der Verarbeitung	Erheben, Empfangen, Speichern, Ordnen, Auslesen, Abfragen, Analysieren, Extrahieren, Klassifizieren, Verknüpfen, Anzeigen, Übermitteln, Drucken und Versenden, Exportieren, Einschränken, Löschen und Archivieren.
Dauer	Laufzeit des Hauptvertrags zuzüglich gesetzlicher Aufbewahrungs- und Nachweisfristen.

Kategorien personenbezogener Daten:

- Konto- und Organisationsdaten: Name, E-Mail-Adresse, gegebenenfalls Firma, Rolle, Einstellungen, Login-Daten in gehashter Form, Passkey-Metadaten.
- Objekt- und Mietverhältnisdaten: Objekte, Einheiten, Flächen, Miteigentumsanteile, Mieten, Vorauszahlungen, Kautionen, Verteilerschlüssel, Zählerstände, Fristen und Erinnerungen.
- Mieterdaten: Name, Anschrift, Kontaktdaten, Bankverbindung der Zahler, Mietzahlungen und Rückstände sowie Inhalte von Mietverträgen, Nachträgen, Übergabeprotokollen und Schriftwechsel.
- Bank- und Transaktionsdaten: Betrag, Datum, Auftraggeber oder Empfänger, IBAN, Verwendungszweck, Zuordnungen, Notizen und vorbereitete Überweisungen.
- E-Mail-Daten: Absender, Empfänger, Betreff, Datum, Text, Anhänge und Metadaten aus weitergeleiteten E-Mails und aus verbundenen Gmail-, Microsoft-365/Outlook- oder IMAP-Postfächern.
- Dokumentdaten: Mietverträge, Rechnungen, Bescheide, WEG-Unterlagen, Versicherungspolicen, Übergabeprotokolle, Fotos (etwa von Zählern), PDF- und Bilddateien, OCR-Daten und Extraktionsergebnisse.
- Telegram- und Kommunikationsdaten: Telegram-User-ID, Chat-ID, Nachrichten, Fotos, Dateien, Sprachnachrichten, Transkripte, Button-Bestätigungen und Support-Kommunikation.
- Schreiben an Mieter: Entwürfe, Empfänger und Anschriften, Freigaben mit Zeitpunkt, Versand- und Zustellstatus sowie optional die Unterschrift des Auftraggebers, die auf seinen Schreiben abgebildet wird.
- Integrationsdaten: OAuth-Tokens, API-Antworten und Fachdaten aus angebundenen Diensten wie Google Drive, Dropbox, Qonto, YAXI/Open Banking, 1Password, Online-Portalen und verbundenen KI-Assistenten.
- Zugangsdaten und Sitzungen: vom Auftraggeber bereitgestellte Portal-Login-Daten, Session-Kontexte, Zwei-Faktor-Hinweise und verschlüsselt gespeicherte Credentials.
- Kontaktdaten Dritter: Handwerker, Versorger, Dienstleister, Hausverwaltungen, WEG-Verwalter, Miteigentümer, Behörden und sonstige Kontakte aus den Unterlagen des Auftraggebers.
- Protokoll-, Diagnose- und Sicherheitsdaten: Zeitstempel, IP-Adressen, Browser- und Gerätedaten, Push-Token der iOS-App, Fehlerlogs, Agent-Aktivitäten und Freigabenachweise.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Ziel der Verarbeitung. Sie können jedoch in vom Auftraggeber bereitgestellten Dokumenten oder Nachrichten enthalten sein, etwa in Schreiben eines Mieters; der Auftraggeber bleibt für die Rechtmäßigkeit dieser Bereitstellung verantwortlich.

Kategorien betroffener Personen:

- Nutzer des Auftraggebers und von ihm eingeladene Personen.
- Mieter, Mitmieter, frühere Mieter, Mietinteressenten, Bürgen und Zahler.
- Handwerker, Versorger, Dienstleister, Hausverwaltungen, WEG-Verwalter und Miteigentümer.
- Absender und Empfänger von E-Mails, Telegram-Nachrichten und Schreiben, soweit deren Daten verarbeitet werden.
- Personen, die in Mietverträgen, Rechnungen, Bescheiden, Protokollen, Kontoumsätzen oder sonstigen Dokumenten des Auftraggebers genannt sind.

Anlage 2: Genehmigte weitere Auftragsverarbeiter

Anbieter	Zweck	Datenarten	Ort / Transfer
Netcup	Hosting und Infrastruktur	Auftraggeber-Daten, Anwendungsdaten, Datenbankdaten	Deutschland
Amazon Web Services (SES)	E-Mail-Versand und Zustellung	E-Mail-Adressen, technische Versanddaten, Inhalte versendeter E-Mails	EU, Irland
Stripe	Zahlungsabwicklung für das Abo des Auftraggebers	Abrechnungsdaten, Zahlungsstatus, Rechnungsdaten	EU/USA, Data Privacy Framework bzw. SCCs
OpenAI	KI-Modelle zum Auslesen von Dokumenten, Bildanalyse, Transkription, für Entwürfe und Antworten des Assistenten	Relevante Eingaben und Dokumentauszüge, keine Nutzung zum Training	USA, Data Privacy Framework bzw. SCCs
Google (Gemini)	KI-Modelle für Bildanalyse und das Auslesen von Dokumenten	Relevante Eingaben und Dokumentauszüge, keine Nutzung zum Training	USA, Data Privacy Framework bzw. SCCs
Anthropic	KI-Modelle (Claude) für Entwürfe und Antworten des Assistenten	Relevante Eingaben und Dokumentauszüge, keine Nutzung zum Training	USA, Data Privacy Framework bzw. SCCs
Browserbase	Browser-Automatisierung zum Abruf von Dokumenten aus Online-Portalen	Portal-URLs, Sitzungskontexte, Seiteninhalte, Screenshots, Dokumente	USA, Data Privacy Framework bzw. SCCs
YAXI	Open-Banking-Anbindung und Abruf von Bankumsätzen nach Einwilligung	Bank- und Transaktionsdaten, Bankverbindungsmetadaten	EU
LetterXpress	Druck und Postversand vom Auftraggeber freigegebener Briefe	Name und Anschrift des Empfängers, Inhalt des Schreibens	Deutschland
PostHog	Produkt- und Fehleranalyse, nur mit Einwilligung	Nutzungs- und Diagnosedaten, pseudonymisierte Nutzerkennungen	USA, Data Privacy Framework bzw. SCCs

Die jeweils aktuelle Anbieterübersicht ist auf der Trust-Seite von Immorento (`https://immorento.de/trust`) abrufbar.

Dienste, die der Auftraggeber selbst verbindet, nutzt der Auftragnehmer nur nach Einrichtung oder Einwilligung des Auftraggebers: Telegram, seine Bank (über YAXI oder die Schnittstelle der Bank, etwa Qonto), Gmail und Google Drive, Microsoft 365/Outlook, Dropbox, IMAP-Server, 1Password, Online-Portale und KI-Assistenten, die er über den MCP-Server von Immorento verbindet. Diese Anbieter verarbeiten die Daten nach ihren eigenen Bestimmungen und sind keine weiteren Auftragsverarbeiter des Auftragnehmers.

Für die Kartendarstellung übermittelt der Auftragnehmer die auf einem Dokument genannte Anschrift des Ausstellers an OpenStreetMap Nominatim (OpenStreetMap Foundation, Vereinigtes Königreich, Angemessenheitsbeschluss), um ihre Koordinaten zu ermitteln.

Anlage 3: Technische und organisatorische Maßnahmen

Die nachfolgenden Maßnahmen beschreiben den Stand zum Stand dieses AVV. Sie werden entsprechend Risiko, Stand der Technik und Produktentwicklung fortlaufend angepasst.

1. Vertraulichkeit

Zugangskontrolle	Betrieb auf kontrollierter Serverinfrastruktur in Deutschland; Administrationszugriff nur für berechtigte Personen; Zugriff auf Produktionssysteme über geschützte Admin-Zugänge.
Zugriffskontrolle	Rollen- und Rechtekonzept, individuelle Nutzerkonten, Passwörter gehasht, optionale Passkeys, Adminzugriff auf das erforderliche Minimum beschränkt.
Mandantentrennung	Mandantenspezifische Datenbankzugriffe, Row-Level-Security und anwendungsseitige Berechtigungsprüfungen.
Verschlüsselung	TLS für Transportwege; verschlüsselte Speicherung sensibler Tokens und Zugangsdaten (Bankzugänge, OAuth-Tokens, Portalzugangsdaten); Trennung von Secrets und Quellcode.

2. Integrität

Weitergabekontrolle	Übermittlungen an weitere Auftragsverarbeiter nur für definierte Zwecke; bevorzugt verschlüsselte Schnittstellen; Zugriff auf verbundene Dienste nur nach Einrichtung oder Einwilligung. Schreiben an Mieter verlassen den Dienst erst nach Freigabe durch den Auftraggeber. Überweisungen bereitet der Dienst nur vor; freigeben kann sie nur der Auftraggeber mit der starken Kundenauthentifizierung seiner Bank.
Eingabekontrolle	Protokollierung relevanter System- und Agentenaktivitäten; Nachvollziehbarkeit von Zuordnungen von Dokumenten und Zahlungen sowie von Freigaben und Versand von Schreiben an Mieter.
Änderungskontrolle	Versionierte Quellcodeverwaltung, Reviews nach Risiko, migrationsbasierte Schemaänderungen und automatisierbare Deployments.
Originale	Vom Auftraggeber oder von Dritten stammende Originaldokumente werden unverändert abgelegt; vom Dienst erstellte Schreiben und Abrechnungen sind als Entwürfe des Auftraggebers gekennzeichnet.

3. Verfügbarkeit und Belastbarkeit

Backups	Regelmäßige Sicherungen von Datenbank und relevanten Systemdaten; Wiederherstellungsprozesse für technische Zwischenfälle.
Monitoring	Systemd-Services, Logs, Fehlerbenachrichtigungen, Job- und Deploy-Überwachung.
Wiederherstellung	Automatisierte Deployments, reproduzierbare Infrastruktur, dokumentierte Betriebsabläufe und Möglichkeit zur Wiederherstellung aus Backups.

4. Regelmäßige Überprüfung

Sicherheitsprüfung	Laufende Pflege von Abhängigkeiten, Fehleranalyse, Zugriffskontrollen und technische Plausibilitätsprüfungen.
Voreinstellungen und Datenminimierung	Datenabruf nur nach Einrichtung oder Einwilligung des Auftraggebers; kein KI-Training mit Auftraggeber-Daten. In der Standardeinstellung werden in verbundenen E-Mail-Postfächern direkt nach dem Verbinden und danach täglich alle neuen E-Mails geprüft, auch gesendete; beim ersten Lauf auch rückwirkend für den gewählten Zeitraum (ohne Auswahl: mindestens die letzten 90 Tage). Ein KI-Modell erhält dabei nur PDF-Anhänge mit Betreff, Absender, Datum und gekürztem E-Mail-Text als Kontext sowie Kaufbeleg-E-Mails ausgewählter Absender (derzeit Apple); importiert werden nur Dokumente, die das Modell als Unterlage des Auftraggebers erkennt, übrige Anhänge werden nicht gespeichert. Zu jeder geprüften E-Mail werden Betreff, Absender und Prüfergebnis protokolliert. Der Auftraggeber kann jedes Postfach jederzeit auf „Nur bei offenen Transaktionen“ umstellen; dann wird es nur gezielt nach Rechnungen zu offenen Bankumsätzen durchsucht.
Unterauftragskontrolle	Auswahl geeigneter Dienstleister, vertragliche Datenschutzpflichten, Transfermechanismen und öffentliche Transparenz über wesentliche Anbieter.