

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 18.10.2026

Vertragsparteien

Verantwortlicher (Auftraggeber): der Kunde von Mailarchiv leicht, wie in seinem Kundenkonto angegeben (im Folgenden „Kunde“)

Auftragsverarbeiter (Auftragnehmer): IDO GmbH, Anderslebener Straße 40, 39387 Oschersleben, vertreten durch den Geschäftsführer Martin Leue, E-Mail info@mailarchiv-leicht.de (im Folgenden „wir“)

Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen von Mailarchiv leicht (§ 9 AGB) und gilt für jedes Kundenkonto, ohne dass er gesondert unterschrieben werden muss. Er wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Die aktuelle Fassung steht unter <https://mailarchiv-leicht.de/avv>; im Kundenkonto steht sie unter „Einstellungen“ als PDF mit den Firmendaten des Kunden bereit.

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch uns im Auftrag des Kunden, wenn er Mailarchiv leicht (mailarchiv-leicht.de) mit einem Kundenkonto nutzt, um seine E-Mails zu archivieren. Den Umfang der Leistungen beschreiben die AGB und die Preisseite. Dazu gehören, je nach Plan:

- das Abholen von E-Mails aus den Postfächern, die der Kunde verbindet (IMAP, nur lesend), und das Empfangen von Kopien über die Journal-Adresse seines Archivs (Journal- oder BCC-Regel seines Mailservers),
- die Übernahme von Altbeständen, die der Kunde hochlädt (PST, MBOX, EML, ZIP),
- die Speicherung der Original-Mails mit Anhängen, verschlüsselt und mit Löschsperre bis zum Ende der vom Kunden gewählten Aufbewahrungsfrist,
- der Suchindex mit Volltext aus Mails und Anhängen, die Anzeige im Browser, das Herunterladen von Originalen und Anhängen und der Export,
- der Prüferzugang für vom Kunden bestimmte Personen (etwa Betriebsprüfer oder Steuerberatung), das Zugriffsprotokoll und die Verfahrensdokumentation.

(2) Nicht Gegenstand dieses Vertrags sind Daten, die wir als eigener Verantwortlicher verarbeiten, zum Beispiel die Zugangs- und Abrechnungsdaten des Kundenkontos, Server-Protokolle, die Reichweitenmessung und Anfragen über das Kontaktformular. Dafür gilt unsere Datenschutzerklärung. Für den Test ohne Konto gelten die Regeln dieses Vertrags entsprechend, soweit der Testende das Postfach eines Unternehmens verbindet.

(3) Der Vertrag gilt, solange das Kundenkonto besteht, und darüber hinaus, solange wir nach Ende des Abos noch Daten des Kunden speichern (§ 9). Pflichten, die ihrer Natur nach über das Vertragsende hinaus gelten, insbesondere zur Löschung und zur Vertraulichkeit, bleiben bestehen.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

(1) **Art der Verarbeitung:** Erheben (Abholen per IMAP, Empfang über die Journal-Adresse, Upload), Speichern, Verschlüsseln, Indexieren, Durchsuchen, Anzeigen, Bereitstellen zum Herunterladen und Exportieren, Bereitstellen für vom Kunden bestimmte Prüfer, Protokollieren und Löschen.

(2) **Zweck:** revisionssichere Aufbewahrung der E-Mails des Kunden zur Erfüllung seiner Aufbewahrungspflichten (insbesondere § 147 AO, § 257 HGB, § 14b UStG) und für seine weiteren geschäftlichen Zwecke sowie deren Wiederauffinden und Bereitstellung.

(3) **Art der Daten:**

- Inhalte der E-Mails: Betreff, Text, Signaturen und Anhänge (zum Beispiel Rechnungen, Verträge, Bilder) mit allen darin enthaltenen Angaben; je nach Inhalt auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, soweit sie in Mails des Kunden vorkommen,
- Metadaten: Absender, Empfänger, Kopie-Empfänger, Datum, Message-ID, Kopfzeilen, Ordner, Postfach, Richtung, Größe und Prüfsummen,
- Zugangsdaten der verbundenen Postfächer (Adresse, Server, Passwort oder App-Passwort),
- Daten der Nutzung des Archivs: Zugriffsprotokoll (wer wann gesucht, angesehen, heruntergeladen oder exportiert hat) und Namen der Personen mit Prüferzugang.

(4) **Betroffene Personen:** Beschäftigte, Organe und Beauftragte des Kunden, deren Postfächer archiviert werden; alle Korrespondenzpartner des Kunden (Kunden, Interessenten, Lieferanten, Dienstleister, Behörden und deren Ansprechpartner) sowie weitere Personen, die in Mails oder Anhängen genannt sind; Personen mit Prüferzugang.

§ 3 Weisungen

(1) Wir verarbeiten die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus diesem Vertrag und aus der Nutzung der Funktionen von Mailarchiv leicht: Was der Kunde im Konto verbindet, hochlädt, einstellt (insbesondere die Aufbewahrungsfrist), sucht, exportiert, freigibt oder löscht, gilt als Weisung. Weitere Weisungen erteilt der Kunde in Textform, etwa per E-Mail an info@mailarchiv-leicht.de. Weisungsberechtigt ist, wer Zugang zum Kundenkonto hat oder den Kunden vertritt.

(2) Die Löschsperre ist Teil der vereinbarten Leistung: Mit der Wahl der Aufbewahrungsfrist weist der Kunde uns an, jede Mail bis zum Ende ihrer Frist unveränderbar zu speichern. Eine Weisung, eine gesperrte Mail vor Fristende zu löschen, können wir technisch nicht ausführen; unlesbar machen lässt sie sich nur durch Vernichtung des Archivschlüssels (§ 9).

(3) Verpflichtet uns das Recht der EU oder Deutschlands zu einer anderen Verarbeitung, teilen wir dem Kunden das vorher mit, sofern das Recht diese Mitteilung nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO). Dazu kann ein Datenzugriff der Finanzbehörde nach § 147 Abs. 6 Satz 2 AO gehören, wenn der Kunde dem Finanzamt mitgeteilt hat, dass seine Daten bei uns liegen.

(4) Halten wir eine Weisung für rechtswidrig, weisen wir den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO).

§ 4 Unsere Pflichten

(1) Wir verarbeiten die Daten ausschließlich, um die vereinbarten Leistungen zu erbringen, nicht für eigene Zwecke, nicht für Werbung und nicht zum Training von KI-Modellen. Inhalte der Mails sehen wir uns nicht an;

ist das ausnahmsweise zur Behebung eines Fehlers nötig, nur auf Anfrage oder mit Zustimmung des Kunden.

(2) Personen, die bei uns Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

(3) Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Wir dürfen sie an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt.

(4) Wir unterstützen den Kunden mit geeigneten Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Art. 12 bis 23 DSGVO). Vieles kann der Kunde selbst im Konto erledigen, etwa alle Mails zu einer Person suchen, ansehen und exportieren. Wenden sich Betroffene direkt an uns, leiten wir die Anfrage unverzüglich an den Kunden weiter.

(5) Wir unterstützen den Kunden bei seinen Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung) im Rahmen der Art der Verarbeitung und der uns vorliegenden Informationen.

(6) Werden uns Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt, melden wir sie dem Kunden unverzüglich per E-Mail an die Adresse seines Kundenkontos, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie uns vorliegen.

(7) Wir verarbeiten die Daten ausschließlich in Deutschland (§ 7).

§ 5 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er bestimmt, welche Postfächer archiviert werden, welche Aufbewahrungsfrist gilt und wer Zugang zum Archiv erhält.

(2) Der Kunde stellt sicher, dass er berechtigt ist, die verbundenen Postfächer archivieren zu lassen. Das gilt insbesondere für Postfächer von Beschäftigten, wenn deren private Nutzung erlaubt ist; der Kunde regelt die private Nutzung, informiert die Beschäftigten und beteiligt, soweit vorhanden, die Arbeitnehmervertretung.

(3) Er gibt Zugangscodes für Prüferzugänge nur an berechtigte Personen weiter und widerruft Zugänge, die nicht mehr gebraucht werden.

(4) Er informiert uns unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde ist mit den in Anlage 2 genannten Unterauftragsverarbeitern einverstanden (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).

(2) Wollen wir einen Unterauftragsverarbeiter hinzunehmen oder ersetzen, informieren wir den Kunden mindestens vier Wochen vorher per E-Mail an die Adresse seines Kundenkontos. Der Kunde kann der Änderung bis zu ihrem Wirksamwerden in Textform widersprechen. Können wir den Einwand nicht ausräumen, kann der Kunde den Vertrag zum Wirksamwerden der Änderung kündigen.

(3) Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO).

(4) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind der Zahlungsdienstleister Stripe, der nur die Daten des Abos verarbeitet und keinen Zugang zum Archiv hat (dafür sind wir selbst Verantwortlicher), sowie die Mailanbieter des Kunden, aus deren Postfächern wir Mails abholen oder die Kopien an die Journal-

Adresse senden; das Verhältnis zu ihnen besteht allein zwischen dem Kunden und seinem Anbieter.

§ 7 Ort der Verarbeitung

Die Verarbeitung findet ausschließlich auf Servern und im Objektspeicher in Rechenzentren in Deutschland statt. Das gilt für das Abholen und Empfangen der Mails, die Speicherung der Originale, eine gegebenenfalls eingerichtete zweite Kopie an einem anderen Standort, den Suchindex, das Zugriffsprotokoll und Exporte. Eine Übermittlung in ein Drittland findet nicht statt. KI-Dienste setzen wir für die Verarbeitung der Mails nicht ein.

§ 8 Nachweise und Kontrollen

(1) Wir weisen die Einhaltung unserer Pflichten in erster Linie durch Auskünfte und Unterlagen nach, etwa die Beschreibung der Maßnahmen in Anlage 1, die Verfahrensdokumentation im Konto und Nachweise unserer Unterauftragsverarbeiter (zum Beispiel das ISO/IEC-27001-Zertifikat der Hetzner Online GmbH für ihre Rechenzentren).

(2) Reicht das nicht aus, kann der Kunde sich nach Anmeldung mit angemessener Frist während der üblichen Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer von der Einhaltung überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Die Kontrolle darf den Betrieb nicht unverhältnismäßig stören und muss die Vertraulichkeit der Daten anderer Kunden wahren. Prüfer, die mit uns im Wettbewerb stehen, dürfen wir ablehnen.

§ 9 Löschung und Rückgabe

(1) Der Kunde kann sein Archiv jederzeit ganz oder gefiltert als ZIP mit den Original-Mails (EML), einem Verzeichnis (CSV) und Prüfsummen exportieren. Das ist die Rückgabe der Daten im Sinne von Art. 28 Abs. 3 lit. g DSGVO.

(2) Jede Mail ist bis zum Ende ihrer Aufbewahrungsfrist technisch gegen Löschen gesperrt (Löschsperre im Compliance-Modus). Vor Fristende kann niemand sie löschen, auch wir nicht.

(3) Endet das Abo, kann der Kunde noch 90 Tage exportieren. Danach vernichten wir den Schlüssel seines Archivs (Krypto-Löschung): Alle Mails, auch etwaige Kopien, sind ab diesem Zeitpunkt für niemanden mehr lesbar. Suchindex, Volltext und Exporte löschen wir dabei sofort. Die verschlüsselten Objekte selbst löschen wir, sobald ihre Löschsperre abgelaufen ist. Löscht der Kunde sein Konto selbst, vernichten wir den Schlüssel sofort.

(4) Im Einzelnen gelten folgende Fristen:

Daten	Löschung
Archivierte Mails mit Anhängen (verschlüsselte Originale)	nach Ende der Aufbewahrungsfrist: 31.12. des Jahres der Mail plus eingestellte Jahre (Standard 10); bis dahin technisch gegen Löschen gesperrt
Ganzes Archiv nach Ende des Abos (Mails, Suchindex, Volltext, Exporte)	90 Tage nach Abo-Ende zum Exportieren, dann Vernichtung des Archivschlüssels (Krypto-Löschung, sofort unlesbar); die verschlüsselten Objekte werden gelöscht, sobald ihre Löschsperre abläuft
Archiv nach einer Testphase ohne Abo	30 Tage nach Ende der Testphase, dann wie oben (Schlüssel vernichtet)
Archiv beim Löschen des Kontos	sofort: Schlüssel vernichtet, Index gelöscht

Daten	Löschung
Zugangsdaten verbundener Postfächer (verschlüsselt)	sobald das Postfach getrennt oder das Archiv vernichtet wird
Export-Dateien (ZIP)	nach 7 Tagen
Hochgeladene Dateien für den Altbestand (PST, MBOX, EML, ZIP)	nach der Verarbeitung
Zugriffsprotokoll des Archivs	solange das Archiv besteht
Prüferzugänge (Name, Zeitraum, Zugangscode nur als Hash)	Zugang endet mit Ablaufdatum oder Widerruf; Eintrag solange das Archiv besteht

§ 10 Haftung und Schlussbestimmungen

- (1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB (§ 10).
- (2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den AGB vor.
- (3) Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Rechenzentrum:** Server und Objektspeicher stehen in Rechenzentren der Hetzner Online GmbH in Deutschland. Zutritt und physische Sicherheit regelt Hetzner; deren Informationssicherheits-Managementsystem ist nach ISO/IEC 27001 zertifiziert (ein Zertifikat von Hetzner, nicht der IDO GmbH). Wir selbst haben keinen physischen Zugang zu den Servern.
- **Zugang zu den Servern:** nur für beauftragte Administratoren der IDO GmbH, nur über verschlüsselte Verbindungen.
- **Verschlüsselung je Archiv:** Jedes Archiv hat einen eigenen, zufällig erzeugten Datenschlüssel. Die Mails liegen damit verschlüsselt im Objektspeicher (XSalsa20-Poly1305, libsodium); eine Veränderung fällt beim Entschlüsseln auf. Der Datenschlüssel liegt nur mit einem Hauptschlüssel verschlüsselt in der Datenbank; der Hauptschlüssel wird getrennt davon aufbewahrt.
- **Postfach-Zugangsdaten:** Passwörter der verbundenen Postfächer speichern wir mit AES-256-GCM verschlüsselt. Auf die Postfächer greifen wir nur lesend und nur über verschlüsselte Verbindungen zu.
- **Anmeldung im Kundenkonto:** Passwort mit mindestens 10 Zeichen, gespeichert nur als Hash (Argon2id). Zwei-Faktor-Anmeldung mit einer Authenticator-App (TOTP) und Notfallcodes. Nach 10 Fehlversuchen in 15 Minuten (je Anschluss und je Konto) ist die Anmeldung gesperrt.
- **Sitzung:** Sitzungs-Cookie nur über HTTPS, für Skripte nicht lesbar (HttpOnly), nicht an fremde Seiten mitgesendet (SameSite), ungültig nach 8 Stunden ohne Aktivität.
- **Trennung:** Jede Abfrage ist an das Archiv des angemeldeten Kontos gebunden, jedes Archiv hat einen eigenen Schlüssel. Unsere Betreiber-Übersicht zeigt Kennzahlen, keine Mailinhalte.
- **Prüferzugang:** nur lesend, auf den freigegebenen Zeitraum beschränkt, befristet und widerrufbar; Link und Zugangscode werden getrennt weitergegeben und nur als Hash gespeichert; die Zahl der Anmeldeversuche ist begrenzt.
- **Transport:** Alle Verbindungen zur Anwendung laufen über HTTPS (TLS) mit HSTS.

Integrität

- **Original unverändert:** Jede Mail wird im Originalformat (EML) gespeichert und mit einer SHA-256-Prüfsumme versehen.
- **Prüfsummen-Kette:** Die Prüfsummen jedes Archivs sind fortlaufend verkettet; eine fehlende oder veränderte Mail fällt auf.
- **Löschsperre:** Speicherung mit Object Lock im Compliance-Modus bis zum Ende der Aufbewahrungsfrist; vor Ablauf kann niemand die Objekte löschen oder überschreiben, auch wir nicht.
- **Integritätsprüfung:** Jede Nacht vergleichen wir Stichproben der Originale mit ihrer Prüfsumme und rechnen die Prüfsummen-Kette jedes Archivs nach.
- **Zugriffsprotokoll:** Suchen, Ansichten, Downloads, Exporte, Prüferzugriffe und Änderungen von Einstellungen werden je Archiv protokolliert; das Protokoll lässt sich in der Anwendung nur fortschreiben, nicht ändern oder löschen.
- **Schutz der Anwendung:** CSRF-Schutz für alle Formulare, strenge Content-Security-Policy, keine Skripte oder Schriften fremder Anbieter, Einbetten in fremde Seiten untersagt, Bot-Schutz ohne externen Dienst.

Verfügbarkeit und Belastbarkeit

- Die Originale liegen im Objektspeicher. Ist eine zweite Kopie an einem anderen Standort eingerichtet, wird jede Mail zusätzlich dorthin geschrieben, ebenfalls mit Löschsperre; fehlende Kopien werden automatisch nachgeholt.
- Vor jeder Aktualisierung der Anwendung wird der neue Stand automatisch geprüft und die Datenbank gesichert. Bei einem Fehler lässt sich der vorherige Stand wiederherstellen.
- Abholung und Pflege der Archive werden überwacht. Störungen eines Postfachs, etwa nach einer Passwortänderung, zeigen wir dem Kunden im Konto an.

Regelmäßige Überprüfung

- Wir überprüfen die Maßnahmen bei jeder wesentlichen Änderung der Anwendung und passen sie an den Stand der Technik an. Unterauftragsverarbeiter setzen wir nur mit Vertrag zur Auftragsverarbeitung ein (Anlage 2).

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Rechenzentrum, Server und Objektspeicher (Hetzner Cloud, Object Storage): Betrieb der Anwendung, der Datenbank mit Suchindex und Protokollen, der Abholung der Mails und Speicherung der verschlüsselten Original-Mails mit Löschsperre; Versand unserer Benachrichtigungsmails über unseren eigenen Mailserver	Deutschland (Rechenzentren Falkenstein und Nürnberg) kein Drittland

Stand dieser Fassung: 18.10.2026