Auftragsverarbeitungsvertrag (AVV / DPA)

Vorlagenversion: 1.1
Ausgestellt: 16. Oktober 2026
Rechtsgrundlage: Verordnung (EU) 2016/679 (DSGVO), Art. 28

> **Hinweis zur Übersetzung.** Deutsche Übersetzung zu Informationszwecken. Rechtlich maßgeblich ist die englische Fassung (`docs/legal/en/DPA-Data-Processing-Agreement.md`); bei Abweichungen gilt die englische Fassung.
> **Haftungsausschluss.** Dies ist die AVV-Vorlage v1.0 gemäß Art. 28 DSGVO. Lassen Sie sich vor der Unterzeichnung von Ihrem eigenen Rechtsbeistand beraten. Cleanthes Apps SRL erteilt keine Rechtsberatung. Platzhalter `{{PLATZHALTER}}` sind bei Unterzeichnung auszufüllen.

---

1. Parteien

1.1. Verantwortlicher (Kunde), nachfolgend „Verantwortlicher":

- Firma: `{{CLIENT_LEGAL_NAME}}`
- Handelsregisternummer / Steuer-ID: `{{CLIENT_CUI}}`
- Sitz: `{{CLIENT_ADDRESS}}`
- Gesetzlicher Vertreter: `{{CLIENT_REPRESENTATIVE}}`, in der Funktion `{{CLIENT_REP_TITLE}}`
- Kontakt-E-Mail: `{{CLIENT_CONTACT_EMAIL}}`
- Datenschutzbeauftragter (DSB), falls benannt: `{{CLIENT_DPO}}`

1.2. Auftragsverarbeiter, nachfolgend „Auftragsverarbeiter":

- Firma: **Cleanthes Apps SRL**
- Handelsregisternummer: `{{CLEANTHES_CUI}}` *(wird nach Eintragung der Gesellschaft ergänzt)*
- Sitz: `{{CLEANTHES_ADDRESS}}` *(ebenso)*
- Gesetzlicher Vertreter: `{{CLEANTHES_REP}}`, in der Funktion `{{CLEANTHES_REP_TITLE}}`
- Datenschutz-Kontakt: `dpo@cleanthes-apps.com`

Gemeinsam als „Parteien", einzeln als „Partei" bezeichnet.

---

2. Gegenstand und Zweck

2.1. Dieser Vertrag regelt die Bedingungen, unter denen der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen im Zusammenhang mit der Software-as-a-Service-Plattform **CAP APP** (der „Dienst") verarbeitet.

2.2. Dieser AVV wird als verbindliche Anlage zum Rahmenvertrag Nr. `{{CONTRACT_NUMBER}}` vom `{{CONTRACT_DATE}}` (der „Hauptvertrag") geschlossen.

2.3. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag in Bezug auf die Verarbeitung personenbezogener Daten geht dieser AVV vor.

---

3. Laufzeit

3.1. Dieser Vertrag tritt am `{{EFFECTIVE_DATE}}` in Kraft und gilt für die gesamte Laufzeit des Hauptvertrags.

3.2. Die Pflichten des Auftragsverarbeiters zu Vertraulichkeit, Löschung und Rückgabe der Daten bestehen nach Beendigung fort.

---

4. Kategorien verarbeiteter personenbezogener Daten

Der Auftragsverarbeiter verarbeitet über den Dienst CAP APP im Auftrag des Verantwortlichen folgende Datenkategorien:

Kategorie	Konkrete Beispiele	Quelle
Identifikation der Mitarbeitenden	Name, Personalnummer, Position, Abteilung	CSV-Import / HRIS-API des Verantwortlichen
Berufliche Kontaktdaten	Geschäftliche E-Mail, geschäftliches Telefon (optional)	Eingabe durch den Verantwortlichen
Berufliche Qualifikationsdaten	Kompetenzen, absolvierte Schulungen, Beginn/Ablauf von Berechtigungen, Bewertungsergebnisse	Eingabe durch den Verantwortlichen / Trainer
Rollen und Berechtigungen	Anwendungsrolle (Mitarbeiter/Trainer/Manager/Admin), Berechtigungen	Konfiguration durch den Verantwortlichen
Technisches Audit-Protokoll	IP-Adresse, User-Agent, Zeitstempel und Art der Aktion	Automatisch durch den Dienst erfasst
Nutzergenerierte Inhalte	PDF-Dokumente (Zertifikate), Profilbilder (optional), Bewertungskommentare	Eingabe durch den Verantwortlichen / Mitarbeitende

Im Regelfall nicht verarbeitet:

- Gesundheitsdaten (außer arbeitsmedizinische Tauglichkeitsbescheinigung, sofern der Verantwortliche diese hochlädt)
- Finanz-/Bankdaten der Mitarbeitenden
- Daten zu politischer, religiöser oder sexueller Orientierung
- Daten zu Vorstrafen

Lädt der Verantwortliche solche Daten hoch, verbleibt die volle Verantwortung für die Rechtsgrundlage beim Verantwortlichen.

---

5. Kategorien betroffener Personen

- Mitarbeitende des Verantwortlichen mit Konto im Dienst (Mitarbeiter, Trainer, Manager, Admin)
- Ehemalige Mitarbeitende des Verantwortlichen, bis zur Löschung des Kontos gemäß Aufbewahrungsrichtlinie
- Gelegentliche Besucher (externer Auditor, Berater) mit temporären, vom Verantwortlichen vergebenen Konten

---

6. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

6.1. **Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten**, einschließlich über die Konfiguration des Dienstes und die Bestimmungen des Hauptvertrags.

6.2. **Die Vertraulichkeit sicherzustellen**: Personal des Auftragsverarbeiters mit Zugriff auf Daten des Verantwortlichen unterzeichnet Vertraulichkeitsverpflichtungen und erhält jährliche DSGVO-Schulungen.

6.3. **Geeignete technische und organisatorische Maßnahmen umzusetzen** (siehe Abschnitt 10).

6.4. **Den Verantwortlichen zu unterstützen** bei der Erfüllung seiner Pflichten in Bezug auf:

- Beantwortung von Anfragen betroffener Personen (Art. 15-22 DSGVO)
- Datenschutz-Folgenabschätzung (DSFA)
- Meldung von Sicherheitsvorfällen

6.5. **Den Verantwortlichen innerhalb von 72 Stunden zu benachrichtigen**, nachdem ein Sicherheitsvorfall mit Bezug auf personenbezogene Daten bekannt wurde, per E-Mail an `{{CLIENT_CONTACT_EMAIL}}` und an `{{CLIENT_DPO}}` (falls benannt).

6.6. **Alle Daten zurückzugeben oder zu löschen** bei Beendigung des Hauptvertrags, gemäß Abschnitt 11.

6.7. **Keine Daten außerhalb des EWR zu übermitteln** ohne Garantien nach Kapitel V DSGVO (Standardvertragsklauseln, Angemessenheitsbeschlüsse).

6.8. **Die Daten nicht für eigene Zwecke zu nutzen** (Marketing, kommerzielle aggregierte Analysen, Training externer KI-Modelle).

---

7. Pflichten des Verantwortlichen

7.1. Der Verantwortliche gewährleistet, dass für die in den Dienst hochgeladenen Daten eine gültige Rechtsgrundlage besteht (Art. 6 DSGVO: in der Regel Durchführung des Arbeitsvertrags oder rechtliche Verpflichtung für Berechtigungen).

7.2. Der Verantwortliche ist für die Konfiguration von Rollen und Berechtigungen im Dienst sowie für den zeitnahen Entzug des Zugriffs ausgeschiedener Mitarbeitender verantwortlich.

7.3. Der Verantwortliche informiert seine Mitarbeitenden gemäß Art. 13-14 DSGVO über die Verarbeitung im Dienst.

7.4. Der Verantwortliche beantwortet direkt bei ihm eingehende Anfragen betroffener Personen. Der Auftragsverarbeiter unterstützt technisch (Export, Löschung) innerhalb von 5 Werktagen.

---

8. Unterauftragsverarbeiter

8.1. Der Verantwortliche erteilt dem Auftragsverarbeiter eine **allgemeine Genehmigung** zur Beauftragung von Unterauftragsverarbeitern, unter folgenden Bedingungen:

- Die Liste der genehmigten Unterauftragsverarbeiter ist in in Anlage 5 zum Hauptvertrag und auf der Trust-Center-Seite der Website veröffentlicht.
- Jeder Unterauftragsverarbeiter schließt mit Cleanthes Apps SRL einen AVV mit Pflichten, die den hier festgelegten gleichwertig sind.

- Der Auftragsverarbeiter informiert den Verantwortlichen mindestens **30 Tage** vor Aufnahme eines neuen Unterauftragsverarbeiters. Der Verantwortliche kann mit Begründung widersprechen; kann der Widerspruch nicht ausgeräumt werden, darf der Verantwortliche ohne Vertragsstrafe kündigen.

8.2. **Aktive Unterauftragsverarbeiter zum Ausstellungsdatum des AVV:**

Unterauftragsverarbeiter	Rolle	Verarbeitungsort	Grundlage der Übermittlung
LowPings Digital Services SRL	Server-Hosting (Anwendung, Datenbank, Dateien, Backups)	Rumänien	EU-Anbieter, keine Übermittlung
Cloudflare Inc.	DNS, CDN und Schutz (der Verkehr läuft verschlüsselt durch ihr Netz)	EU / globales Netz	SCC + Cloudflare EU-DPA
Stripe Payments Europe Ltd	Kartenzahlung (Abonnement und KI-Guthabenpakete)	Irland (EU)	EU-Anbieter, keine Übermittlung
Anthropic, PBC	KI-Funktionen: Lesen von Dokumenten, erzeugte Tests, Assistent (optional, standardmäßig aus)	USA	SCC über den AVV von Anthropic (nur wenn für den Kunden eingeschaltet)

Hinweis: Der Anbieter für Transaktions-E-Mails (Benachrichtigungen, Passwort-Reset) wird in der EU gewählt und mit der 30-tägigen Ankündigung nach Art. 8.1 in die Liste aufgenommen. Derzeit nutzen wir keine externe Fehlerüberwachung.

---

9. Internationale Datenübermittlung

9.1. Verarbeitete Daten verbleiben in der **Europäischen Union** (Server: Rumänien, LowPings).

9.2. Übermittlungen in die USA (nur die KI-Funktionen, falls eingeschaltet, und Cloudflare) stützen sich auf:

- Standardvertragsklauseln (SCC) gemäß Beschluss (EU) 2021/914
- Ergänzende technische Maßnahmen: es wird nur gesendet, was der Vorgang braucht, TLS 1.2+ bei der Übertragung

9.3. Der Verantwortliche erhält auf Anfrage eine Kopie der mit US-Unterauftragsverarbeitern unterzeichneten SCC.

---

10. Technische und organisatorische Sicherheitsmaßnahmen

10.1. **Authentifizierung und Autorisierung:**

- Passwörter mit bcrypt gehasht (Kostenfaktor 12+)
- Zwei-Schritt-Anmeldung (Authenticator-App) verpflichtend für Plattform-Administratoren; SAML-SSO mit dem Firmenkonto im Enterprise-Plan
- Sitzungen mit Ablauf, ungültig bei Abmeldung, Passwortänderung und mit „Von allen Geräten abmelden“
- Strikte Trennung zwischen Kunden: jede Anfrage sieht nur die Daten ihres Kunden, durch automatische Tests geprüft

10.2. **Verschlüsselung:**

- Bei der Übertragung: HTTPS/TLS 1.2+ verpflichtend, HSTS aktiv
- Passwörter und PINs werden nur als Hash (bcrypt) gespeichert, nie im Klartext
- Geheimnisse (API-Schlüssel, DB-Passwörter) verschlüsselt gespeichert, nicht in Git

10.3. **Audit-Protokoll:**

- Alle kritischen CRUD-Aktionen werden protokolliert: wer, was, wann, von welcher IP
- Aufbewahrung der Protokolle: mindestens 12 Monate

10.4. **Backup und Wiederherstellung:**

- Tägliches automatisches Backup (Datenbank, Dateien, Konfiguration)
- Aufbewahrung 90 Tage, auf der Infrastruktur des Dienstes in Rumänien; eine Kopie außerhalb des Hauptservers folgt später, mit Mitteilung an den Verantwortlichen
- Dokumentiertes Wiederherstellungsverfahren; Wiederherstellungstest auf Anfrage
- RTO: 24 Stunden | RPO: 24 Stunden

10.5. **Personalzugriff:**

- Prinzip der minimalen Rechte
- Zugriffsprotokolle werden überwacht
- Zugriff wird innerhalb von 24 h nach Ende der Zusammenarbeit entzogen

10.6. **Sicherheitstests:**

- Abhängigkeiten werden automatisch geprüft (Dependabot / Renovate)
- Jährlicher Penetrationstest geplant *(erste Kampagne: Q2 2027, nach 5 Live-Kunden)*
- Responsible Disclosure (auf der Website veröffentlichte Richtlinie)

---

11. Aufbewahrung und Löschung der Daten

11.1. **Während der Vertragslaufzeit:** Der Auftragsverarbeiter bewahrt die Daten gemäß Konfiguration des Verantwortlichen auf.

11.2. **Standard-Aufbewahrungsrichtlinie:**

- Audit-Protokolle (Aktionsprotokolle): rollierend 12 Monate
- Backups: 90 Tage
- Vom Verantwortlichen deaktiviertes Konto: 30 Tage Karenz, danach Anonymisierung

11.3. **Bei Vertragsende:**

- Der Verantwortliche kann seine Daten 30 Tage lang exportieren (CSV / PDF / JSON)
- Nach diesen 30 Tagen werden die Daten endgültig aus der Produktion gelöscht, mit vorheriger E-Mail-Warnung
- Backups laufen innerhalb von 90 Tagen natürlich aus
- Löschbescheinigung auf Anfrage

11.4. Der Verantwortliche kann eine vorzeitige Löschung schriftlich an `dpo@cleanthes-apps.com` beantragen.

---

12. Rechte der betroffenen Personen

12.1. Anfragen betroffener Personen sind primär an den Verantwortlichen zu richten. Der Auftragsverarbeiter unterstützt technisch:

- Export personenbezogener Daten (Art. 15 Auskunft / Art. 20 Übertragbarkeit): Lieferung innerhalb von 5 Werktagen
- Berichtigung unrichtiger Daten: sofort wirksam (der Verantwortliche ändert über die Oberfläche)
- Löschung (Art. 17): innerhalb von 30 Tagen wirksam
- Einschränkung / Widerspruch. Der Auftragsverarbeiter sperrt den Kontozugriff auf Anfrage des Verantwortlichen

12.2. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage an den Verantwortlichen weiter und informiert die betroffene Person innerhalb von 5 Werktagen.

---

13. Prüfrechte

13.1. Der Verantwortliche kann die Einhaltung durch den Auftragsverarbeiter überprüfen:

- Über einen jährlichen Sicherheitsfragebogen (Antwort des Auftragsverarbeiters innerhalb von 30 Tagen)
- Über Dokumentenanforderung (Security Whitepaper, Compliance-Matrix, Pentest-Bericht sobald verfügbar)
- Über eine Vor-Ort-Prüfung mit 60 Tagen Vorankündigung, zu Geschäftszeiten, Kosten trägt der Verantwortliche (sofern die Prüfung keine wesentlichen Verstöße feststellt)

13.2. Der Auftragsverarbeiter kann stattdessen Prüfberichte Dritter vorlegen (z. B. ISO 27001): *diese Zertifizierung ist in Vorbereitung, geplant für 2027. Bis dahin: Security Whitepaper + Compliance-Matrix + Beantwortung des Fragebogens.*

---

14. Überprüfung

14.1. Dieser AVV wird jährlich oder bei Änderungen des anwendbaren Rechts überprüft.

14.2. Für den Verantwortlichen nachteilige Änderungen werden mindestens 90 Tage im Voraus mitgeteilt. Der Verantwortliche kann in diesem Zeitraum ohne Vertragsstrafe kündigen.

---

15. Anwendbares Recht und Gerichtsstand

15.1. Dieser AVV unterliegt dem Recht Rumäniens und der DSGVO.

15.2. Streitigkeiten werden gütlich beigelegt; andernfalls sind die Gerichte in **Timișoara, Rumänien** zuständig.

15.3. Betroffene Personen können Beschwerde bei der **ANSPDCP** (rumänische Datenschutzbehörde), https://www.dataprotection.ro, oder bei der für sie zuständigen Aufsichtsbehörde einlegen.

---

16. Unterschriften

Verantwortlicher:

Name: `{{CLIENT_REPRESENTATIVE}}`
Funktion: `{{CLIENT_REP_TITLE}}`
Datum: `{{SIGNATURE_DATE}}`

Unterschrift + Stempel: `{{CLIENT_SIGNATURE}}`

Auftragsverarbeiter: Cleanthes Apps SRL

Name: `{{CLEANTHES_REP}}`
Funktion: `{{CLEANTHES_REP_TITLE}}`
Datum: `{{SIGNATURE_DATE}}`

Unterschrift + Stempel: `{{CLEANTHES_SIGNATURE}}`

Ausgefertigt in zwei Originalen, eines für jede Partei.
AVV-Vorlage v1.0, 28. August 2026, Cleanthes Apps SRL. Deutsche Übersetzung zu Informationszwecken; rechtlich maßgeblich ist die englische Fassung.