Vertrag zur Auftragsverarbeitung

gem. Art. 28 DSGVO

Version 1.0 vom 22. April 2026

Zwischen

Auftraggeber (Verantwortlicher)	Auftragnehmer (Auftragsverarbeiter)
Der jeweilige Kunde, der das Bewerbermanagement-Tool unter app.rankingdocs.de nutzt (nachfolgend: Auftraggeber)	**Rankingdocs GmbH** Spohrstr. 2 22083 Hamburg Deutschland Vertreten durch: Sebastian Weidner, René Ramcke E-Mail: kontakt@rankingdocs.de

§ 1 Präambel

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer (nachfolgend gemeinsam "Parteien") im Rahmen der Verarbeitung personenbezogener Daten im Auftrag gem. Art. 28 DSGVO.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

(3) Mit der Nutzung des Bewerbermanagement-Tools unter app.rankingdocs.de akzeptiert der Auftraggeber die Bedingungen dieses Vertrags. Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) und des Dienstleistungsvertrags zwischen den Parteien.

§ 2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers personenbezogene Daten im Rahmen des webbasierten Bewerbermanagement-Tools (app.rankingdocs.de). Dies umfasst die Erfassung, Speicherung, Organisation, Verwaltung und Löschung von Bewerberdaten, die über verschiedene Online-Kanäle generiert werden.

2.2 Dauer

Die Verarbeitung beginnt mit der Erstellung eines Kundenkontos und erfolgt auf unbestimmte Zeit bis zur Kündigung des Hauptvertrags oder dieses Vertrags durch eine der Parteien.

§ 3 Art, Zweck und betroffene Personen

3.1 Art der Verarbeitung

Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Auslesen, Abfragen, Verwendung, Übermittlung (per E-Mail-Benachrichtigung), Einschränkung, Löschung und Vernichtung von Daten.

3.2 Zweck der Verarbeitung

Bewerbermanagement im Auftrag des Auftraggebers. Der Auftragnehmer stellt dem Auftraggeber ein Tool zur Verfügung, mit dem eingehende Bewerbungen verwaltet, bewertet und weiterverarbeitet werden können.

3.3 Art der personenbezogenen Daten

Datenkategorie	Konkrete Daten
Kontaktdaten Bewerber	Name, Vorname, E-Mail-Adresse, Telefonnummer
Bewerbungsdaten	Lebenslauf (PDF), Berufserfahrung, Ausbildung, Sprachniveau, gewünschte Stelle, Verfügbarkeit, Erreichbarkeit, Arbeitserfahrung
Kommunikationsdaten	Notizen, Beschreibungen, Verlaufs-/Statuseinträge, Bewertungen
Zugangsdaten Kunden	Name, E-Mail-Adresse, gehashte Passwörter, Login-Zeitpunkte

3.4 Kategorien betroffener Personen

- Bewerber/Kandidaten, die sich über Online-Kanäle (z. B. Landbot-Chatbot) beworben haben
- Mitarbeiter und Zugriffsberechtigte des Auftraggebers (Kunden-Portal-User)

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglichen Vereinbarung und nach Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet.

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, sind zur Vertraulichkeit verpflichtet.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrung der Rechte betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) im erforderlichen Umfang.

§ 5 Sicherheit der Verarbeitung

(1) Die technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO sind in Anlage 1 festgelegt.

(2) Die Maßnahmen können der technischen Weiterentwicklung angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Die im Auftrag verarbeiteten Daten werden von sonstigen Datenbeständen strikt getrennt (mandantenfähige Architektur mit Row-Level-Security).

§ 6 Löschung und Rückgabe von Daten

(1) Der Auftragnehmer löscht im Auftrag verarbeitete Daten nach Weisung des Auftraggebers oder nach Ablauf der konfigurierten Löschfristen automatisiert.

(2) Das Bewerbermanagement-Tool bietet dem Auftraggeber jederzeit die Möglichkeit, Daten eigenständig zu exportieren (DSGVO-Export-Funktion) und zu löschen.

(3) Nach Beendigung des Vertragsverhältnisses werden alle personenbezogenen Daten des Auftraggebers innerhalb von 30 Tagen unwiderruflich gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Unterauftragsverarbeiter gem. Anlage 2 einzusetzen, sofern diese vertraglich mindestens vergleichbare Datenschutzpflichten übernommen haben.

(2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Bezug auf Unterauftragsverarbeiter. Der Auftraggeber hat das Recht, gegen den Einsatz neuer Unterauftragsverarbeiter Einspruch zu erheben.

(3) Die aktuell genehmigten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Datenschutzvorschriften beim Auftragnehmer in angemessenem Umfang zu überprüfen.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.

(3) Kontrollen finden nach angemessener Vorankündigung und nicht häufiger als einmal jährlich statt, sofern kein begründeter Verdacht auf einen Verstoß besteht.

§ 9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung mit.

(2) Die Mitteilung umfasst eine Beschreibung der Art der Verletzung, die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie ergriffene Gegenmaßnahmen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gem. Art. 33 und 34 DSGVO.

§ 10 Weisungen

(1) Der Auftraggeber erteilt Weisungen in der Regel über die Funktionen des Bewerbermanagement-Tools. Ergänzende Weisungen können schriftlich per E-Mail an kontakt@rankingdocs.de erteilt werden.

(2) Der Auftragnehmer macht den Auftraggeber darauf aufmerksam, wenn eine Weisung seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die eine betroffene Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung erleidet, haften Auftraggeber und Auftragnehmer gem. Art. 82 DSGVO.

(2) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die durch vorsätzliche oder grob fahrlässige Verstöße gegen diesen Vertrag oder die DSGVO entstehen.

§ 12 Laufzeit und Kündigung

(1) Dieser Vertrag gilt für die Dauer des Hauptvertrags (Dienstleistungsvertrag/AGB).

(2) Der Auftraggeber kann diesen Vertrag jederzeit außerordentlich kündigen, wenn der Auftragnehmer wesentlich gegen Datenschutzpflichten verstößt oder Kontrollrechte verweigert.

(3) Bei Beendigung gelten die Regelungen zur Löschung gem. § 6.

§ 13 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, bleibt die Wirksamkeit des Vertrags im Übrigen unberührt.

(2) Änderungen dieses Vertrags bedürfen der Schriftform.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Technische und organisatorische Maßnahmen

Der Auftragnehmer hat folgende Maßnahmen gem. Art. 32 DSGVO implementiert:

Hosting und Infrastruktur

- Die Anwendung wird auf Servern in der EU (Frankfurt am Main, Region eu-central-1) gehostet.
- Die Datenbank (PostgreSQL) wird bei Supabase auf AWS eu-central-1 (Frankfurt) betrieben.
- Das Frontend und die Serverless Functions werden über Vercel (Region Frankfurt) bereitgestellt.
- Alle Datenübertragungen erfolgen TLS-verschlüsselt (HTTPS).

Zugangs- und Zugriffskontrolle

- Authentifizierung über Supabase Auth mit gehashten Passwörtern (bcrypt).
- Rollenbasierte Zugriffskontrolle (Admin, Kunden-Portal-User) mit serverseitiger Prüfung.
- Row-Level-Security (RLS) auf Datenbankebene für mandantenfähige Datentrennung.
- Ownership-Checks auf allen Mutations-Operationen (Statusänderungen, Notizen, etc.).
- Webhook-Endpunkte sind durch Secret-Token-Validierung geschützt.
- Administratorenzugang ist auf das Notwendigste begrenzt.

Eingabekontrolle

- Alle Datenänderungen werden im Aktivitäts-Verlauf protokolliert (Benutzer, Zeitpunkt, Aktion).
- Automatisches Error-Monitoring über Sentry mit Echtzeit-Benachrichtigungen.

Trennungskontrolle

- Mandantenfähige Architektur: Jeder Kunde sieht ausschließlich seine eigenen Daten.
- Daten verschiedener Kunden werden logisch getrennt gespeichert und über Zugehörigkeits-IDs abgesichert.
- Kampagnen-Zugriffe werden pro Portal-User individuell konfiguriert.

Verfügbarkeit und Belastbarkeit

- Hosting auf hochverfügbarer Cloud-Infrastruktur (AWS/Vercel) mit automatischer Skalierung.
- Regelmäßige Datenbank-Backups (bei Supabase Pro: tägliche Point-in-Time-Recovery-Backups).

Datenlöschung

- Konfigurierbare Löschfristen pro Kampagne.
- Automatisierter täglicher Cron-Job zur Löschung abgelaufener Daten.
- DSGVO-Export-Funktion für betroffene Personen.
- Manuelle Löschung jederzeit durch den Auftraggeber möglich.

E-Mail-Kommunikation

- Transaktionale E-Mails werden über Resend versendet (Absender: noreply@rankingdocs.de, verifizierte Domain).
- Kein Einsatz von Marketing-Cookies, Tracking-Pixeln oder Analyse-Tools.

Anlage 2 – Zugelassene Unterauftragsverarbeiter

Folgende Unterauftragsverarbeiter sind vom Auftraggeber genehmigt:

Unternehmen	Serverstandort	Auftragsinhalt	DPA
Supabase Inc. (auf AWS)	Frankfurt, Deutschland (eu-central-1)	Datenbank, Authentifizierung, Datei-Storage, Realtime	supabase.com/legal/dpa
Vercel Inc.	Frankfurt, Deutschland (fra1)	Hosting der Webanwendung, Serverless Functions, Cron Jobs	vercel.com/legal/dpa
Resend Inc.	USA (mit DPA)	Versand transaktionaler E-Mails (Benachrichtigungen, Einladungen)	resend.com/legal/dpa
Sentry (Functional Software Inc.)	USA (mit DPA)	Error-Monitoring und Performance-Überwachung	sentry.io/legal/dpa

Hinweis: Alle Unterauftragsverarbeiter mit Sitz in den USA verfügen über einen Data Processing Agreement (DPA) und/oder sind unter dem EU-U.S. Data Privacy Framework zertifiziert. Die Kerndaten (Datenbank, Dateien) werden ausschließlich in der EU (Frankfurt am Main) gespeichert.

Anlage 3 – Weisungsberechtigte Personen

Auftragnehmer (Entgegennahme von Weisungen):

Sebastian Weidner

Geschäftsführer

E-Mail: kontakt@rankingdocs.de

Kontakt zur Meldung von Datenschutzverletzungen:

Sebastian Weidner

E-Mail: kontakt@rankingdocs.de

Anlage 4 – Datenschutzbeauftragter

Beim Auftragnehmer wurde gem. § 38 Abs. 1 S. 1 BDSG kein Datenschutzbeauftragter bestellt, da die Anzahl der ständig mit der automatisierten Verarbeitung beschäftigten Personen unter 20 liegt.