Auftragsverarbeitungsvertrag (AVV)

Version 2026-09-09-demo14 · SHA-256: b34e194c412b…

Entwurf
Juristisch ungeprüfter Entwurf — nicht für den Produktivbetrieb bestimmt.

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO für Richaard

Auftragsverarbeiter: Nikita Erochok, Einzelunternehmer, Feierabendweg 23, 44799 Bochum, Deutschland

Verantwortlicher: der jeweilige Kunde von Richaard (Unternehmen / Recruiter)

Stand: 9. September 2026

Version: 2026-09-09-demo14 – 14-tägige Demo und Anlagen A bis D

> *Wichtiger Hinweis (Entwurf, keine Rechtsberatung)*
> *Diese Fassung beschreibt die eingesetzten Produktionssysteme und enthält die Anlagen A (TOMs), B (Dienstleister), C (Weisungen und Unterstützung) und D (Rückgabe und Löschung). Sie ist juristisch noch nicht abschließend geprüft. Offene organisatorische Nachweise und anbieterseitige Aufbewahrungsfristen sind ausdrücklich benannt; sie werden nicht als bereits erfüllte Maßnahmen zugesichert. Die elektronische Annahme in der App umfasst den Vertrag und sämtliche Anlagen.*

Präambel

Der Kunde (Verantwortlicher) nutzt den Dienst **Richaard**, um Bewerbungsunterlagen und Stelleninformationen zu verarbeiten. Der Anbieter (Auftragsverarbeiter) verarbeitet diese Daten ausschließlich im Auftrag und nach Weisung des Kunden. Kontodaten des Kunden selbst fallen **nicht** unter diesen AVV (dort ist der Anbieter eigener Verantwortlicher; siehe [gemeinsame Datenschutzerklärung](https://richaard.de/datenschutz)).

Dieser Vertrag konkretisiert die Pflichten der Parteien nach Art. 28, 32–36 DSGVO.

---

§ 1 Gegenstand, Dauer, Art und Zweck

(1) **Gegenstand:** Bereitstellung der Software **Richaard** als SaaS zur Unterstützung des Kunden bei der internen Recruiting-Auswahl, einschließlich Speicherung und Nutzung von Bewerbungs- und Stellendaten im Auftrag des Kunden.

(2) **Dauer:** für die Laufzeit des Nutzungsvertrags (AGB) zuzüglich der Nachlaufzeit für Löschung/Rückgabe nach § 10.

(3) **Art der Verarbeitung:** Erheben, Speichern, Auslesen, Organisieren, Abgleichen, Übermitteln an Unterauftragsverarbeiter, soweit für den Betrieb erforderlich, KI-gestütztes Bewerten, Anzeigen, Löschen. Keine Emotionserkennung, kein Social Scoring, keine eigene Einstellungs- oder Absageentscheidung durch den Auftragsverarbeiter.

(4) **Zweck:** Unterstützung des Kunden bei der internen Recruiting-Auswahl. Auftragsdaten werden weder für eigene Werbung noch zum eigenen Modelltraining genutzt. Gemini wird über Google Cloud / Vertex AI mit der konfigurierten Region EU eingesetzt. Google beschreibt für diesen Dienst, dass Kundendaten ohne vorherige Erlaubnis oder Anweisung nicht zum Training oder zur Feinabstimmung seiner Modelle verwendet werden. Eine solche Erlaubnis wird im beschriebenen Betrieb nicht erteilt. Sicherheits- und Missbrauchsprüfungen können nach den Google-Bedingungen eine vorübergehende Verarbeitung und Speicherung einschließen; eine pauschale Zusicherung von „Zero Data Retention“ wird nicht abgegeben. Die öffentliche Gemini-Verbraucheranwendung und die Gemini Developer API sind nicht der hier vereinbarte Produktionspfad.

(5) **Weisungen:** Die dokumentierten Weisungen ergeben sich aus diesem AVV, den AGB, der Nutzung der Oberfläche (Uploads, Löschaktionen) und gesonderten Weisungen in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

---

§ 2 Kategorien betroffener Personen

- Bewerberinnen und Bewerber / Kandidatinnen und Kandidaten, deren Unterlagen der Kunde hochlädt
- ggf. in Lebensläufen genannte Dritte (Referenzen, frühere Vorgesetzte)

• Beschäftigte des Kunden, soweit sie den Dienst bedienen (nur insoweit deren Handlungen in Auftragsdaten einfließen; Accountdaten selbst außerhalb dieses AVV)

---

§ 3 Arten personenbezogener Daten

Je nach Inhalt der hochgeladenen Dateien insbesondere:

- Identifikations- und Kontaktdaten (Name, Anschrift, E-Mail, Telefon)
- Bewerbungsfoto, soweit im PDF enthalten
- Berufs- und Ausbildungsdaten, Zeugnisse, Skills, Gehaltsvorstellungen
- Anschreiben, Links, Arbeitserlaubnis-/Verfügbarkeitsangaben
- vom System erzeugte Ableitungen: extrahierter Text, Profile, Embeddings, Scores, Rankings, Chat-Protokolle zum Matching
- **besondere Kategorien** nach Art. 9 Abs. 1 DSGVO, **falls** der Kunde solche Daten hochlädt (Gesundheit, Religion, Gewerkschaft, sexuelle Orientierung, ethnische Herkunft, biometrische Daten, soweit sie zur eindeutigen Identifizierung verarbeitet werden). Der Auftragsverarbeiter fordert solche Daten nicht aktiv an. Der Kunde darf sie nur hochladen, wenn eine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegt.

Ein gewöhnliches Bewerbungsfoto ist nicht allein deshalb ein biometrisches Datum zur eindeutigen Identifizierung.

Stellenausschreibungen können personenbezogene Daten enthalten, wenn sie identifizierbare Ansprechpersonen nennen.

---

§ 4 Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3)

Der Auftragsverarbeiter

a) verarbeitet personenbezogene Daten **nur auf dokumentierte Weisung**, einschließlich Übermittlungen in Drittländer, es sei denn Unions- oder Mitgliedstaatenrecht verpflichtet ihn; dann Information des Kunden, soweit das Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses verbietet;

b) stellt sicher, dass zur Verarbeitung befugte Personen zur **Vertraulichkeit** verpflichtet sind oder einer gesetzlichen Verschwiegenheit unterliegen;

c) trifft alle Maßnahmen nach **Art. 32 DSGVO** (Anlage A – TOMs);

d) hält die Bedingungen für die Inanspruchnahme weiterer Auftragsverarbeiter nach § 7 ein;

e) unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten (Kapitel III DSGVO);

f) unterstützt bei Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, DSFA, vorherige Konsultation), soweit die Informationen beim Auftragsverarbeiter vorhanden sind;

g) löscht oder gibt nach Wahl des Kunden nach Ende der Verarbeitungstätigkeit alle Daten zurück und löscht vorhandene Kopien, sofern kein gesetzlicher Speichergrund entgegensteht;

h) stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Artikels zur Verfügung und ermöglicht **Prüfungen (Audits)** einschließlich Inspektionen durch den Kunden oder einen beauftragten Prüfer (§ 9).

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, **informiert er den Kunden unverzüglich** (Art. 28 Abs. 3 Unterabs. 3 DSGVO) und darf die Ausführung bis zur Klärung aussetzen.

---

§ 5 Pflichten des Verantwortlichen

(1) Der Kunde ist allein für die Rechtmäßigkeit der Übermittlung an Richaard verantwortlich (Rechtsgrundlage Art. 6, ggf. Art. 9 DSGVO; Information der Betroffenen nach Art. 13/14; AGG; Betriebsverfassung).

(2) Der Kunde erteilt nur rechtmäßige Weisungen und nutzt die Löschfunktionen, sobald Daten nicht mehr erforderlich sind (Bewerbungsfristen).

(3) Der Kunde führt, soweit Art. 35 DSGVO es verlangt, eine Datenschutz-Folgenabschätzung für KI-gestütztes Recruiting durch. Der Auftragsverarbeiter leistet angemessene Unterstützung (Art. 28 Abs. 3 lit. f).

---

§ 6 Ort der Verarbeitung, Drittländer

(1) Cloud Run und Cloud Storage sind in Belgien konfiguriert, die Neon-Datenbank in Frankfurt und die KI-Verarbeitung mit der Region EU. Cloudflare verarbeitet App-Anfragen im globalen Netzwerk. Plattformprotokolle, Support und Unterauftragsverhältnisse der Anbieter können weitere Verarbeitungsorte einschließen. Die Angaben in Anlage B beschreiben die jeweilige Funktion; eine ausschließlich europäische Verarbeitung sämtlicher Daten wird nicht zugesichert.

(2) Für Übermittlungen außerhalb des EWR müssen die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sein. Maßgeblich sind ein anwendbarer Angemessenheitsbeschluss oder geeignete Garantien, insbesondere die EU-Standardvertragsklauseln mit erforderlichen ergänzenden Maßnahmen. Eine Nutzung des EU-US Data Privacy Framework setzt voraus, dass der konkrete Empfänger und die betroffene Verarbeitung von einer wirksamen Zertifizierung erfasst sind. EU-Hosting ersetzt diese Prüfung nicht.

(3) Der Auftragsverarbeiter dokumentiert die einschlägigen Verträge, Empfänger und Transfergarantien und stellt dem Kunden die erforderlichen Informationen zur Verfügung. Die allgemeine Genehmigung nach § 7 ersetzt weder diesen Nachweis noch eine erforderliche Prüfung der Drittlandübermittlung. Kann eine Verarbeitung nicht rechtmäßig durchgeführt werden, wird sie ausgesetzt; die Parteien klären eine datenschutzgerechte Alternative oder die Beendigung des betroffenen Leistungsteils.

---

§ 7 Unterauftragsverarbeiter (Art. 28 Abs. 2 und 4)

(1) Der Kunde erteilt die **allgemeine schriftliche Genehmigung** (einschließlich elektronischer Form), Unterauftragsverarbeiter einzusetzen.

(2) Die zum Vertragsbeginn eingesetzten Unterauftragsverarbeiter ergeben sich aus **Anlage B**.

(3) Der Auftragsverarbeiter unterrichtet den Kunden über beabsichtigte Hinzufügungen oder Ersetzungen **vorab** (Art. 28 Abs. 2 Satz 2), mit einer Widerspruchsfrist von **14 Tagen**. Bei begründetem Widerspruch (Datenschutzrisiko) bemühen sich die Parteien um eine Lösung. Scheitert sie, darf der Kunde den betroffenen Leistungsteil oder den Vertrag kündigen.

(4) Mit jedem Unterauftragsverarbeiter werden im Wesentlichen dieselben Datenschutzpflichten vereinbart. Der Auftragsverarbeiter bleibt gegenüber dem Kunden für die Erfüllung durch den Unterauftragsverarbeiter verantwortlich (Art. 28 Abs. 4 Satz 2).

(5) Keine Genehmigung für Unterauftragsverarbeiter, die ohne Kapitel-V-Grundlage in unsichere Drittländer übermitteln.

---

§ 8 Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter unterrichtet den Kunden **unverzüglich**, ohne schuldhaftes Zögern nach Bekanntwerden einer Verletzung nach Art. 4 Nr. 12 DSGVO, mit den nach Art. 33 Abs. 3 verfügbaren Angaben, damit der Kunde Art. 33/34 einhalten kann. Die Meldepflicht gegenüber der Aufsicht bleibt beim Verantwortlichen, soweit dieser Verantwortlicher ist.

---

§ 9 Nachweis und Audits

(1) Der Auftragsverarbeiter stellt auf Anfrage geeignete Nachweise bereit (z. B. aktuelle TOM-Beschreibung, Zertifikate von Subprozessoren, soweit vorhanden, Auszüge aus AV-Verträgen ohne Geschäftsgeheimnisse Dritter).

(2) Prüfungen werden grundsätzlich mit angemessener Vorankündigung und möglichst ohne Beeinträchtigung des Betriebs vereinbart. Bei Datenschutzvorfällen, konkreten Zweifeln an der Einhaltung oder behördlichen Anforderungen sind auch kurzfristige und zusätzliche Prüfungen möglich. Gesetzliche Kontrollrechte werden nicht durch eine starre Häufigkeits- oder Ankündigungsgrenze beschränkt.

(3) Der Kunde trägt eigene Kosten; Kosten des Auftragsverarbeiters bei offensichtlich unbegründeten oder exzessiven Audits kann dieser in angemessenem Umfang verlangen. Behördliche Prüfungen bleiben unberührt.

(4) Als Einzelunternehmer ohne eigenes Rechenzentrum erfolgt die Prüfung der Infrastruktur vorrangig über Nachweise der Subprozessoren (Google, Datenbankhost).

---

§ 10 Rückgabe und Löschung

(1) Rückgabe und Löschung richten sich nach der dokumentierten Wahl und den Weisungen des Kunden. Der Kunde kann verfügbare Lösch- und Downloadfunktionen der Anwendung nutzen; für vollständige Rückgabe, Löschung oder Einschränkung wendet er sich an kontakt@richaard.de. Eine fehlende Schaltfläche beschränkt seine vertraglichen Rechte nicht.

(2) Nach Ende der Verarbeitung gibt der Auftragsverarbeiter die Auftragsdaten nach Wahl des Kunden zurück und löscht die verbleibenden Kopien oder löscht die Daten ohne vorherige Rückgabe. Eine gesetzliche Speicherpflicht bleibt vorbehalten und wird dem Kunden unter Angabe des Grundes mitgeteilt. Einzelheiten einschließlich Profilen, Embeddings, Sitzungen und Sicherungskopien regelt Anlage D. Eigene wirtschaftliche Interessen begründen kein pauschales Zurückbehalten der Auftragsdaten.

(3) Die automatische Löschung im Trial erfolgt nach Anlage D. Der Kunde bewahrt die von ihm benötigten Originale deshalb zusätzlich selbst auf. Die Dateiregel ersetzt nicht die vollständige Löschung des Datenbestands und beseitigt nicht die Pflichten aus Absatz 2.

---

§ 11 Haftung

Die Haftung der Parteien gegenüber Betroffenen richtet sich nach Art. 82 DSGVO. Im Innenverhältnis gelten die AGB, unbeschadet zwingenden Datenschutzrechts. Bußgelder nach Art. 83 trägt jede Partei, soweit sie ihr zurechenbar sind.

---

§ 12 Laufzeit, Kündigung, Vorrang

(1) Der AVV beginnt mit Einbeziehung (Checkbox/Klickwrap oder Unterzeichnung) und endet mit vollständiger Löschung nach § 10, jedoch nicht vor Ende des Hauptvertrags hinsichtlich der Verarbeitungspflicht.

(2) Bei Widerspruch zwischen AGB und AVV geht für Datenschutzfragen der Auftragsverarbeitung dieser AVV vor.

(3) Wesentliche Änderungen werden als neue Fassung dokumentiert und dem Kunden zur Vereinbarung vorgelegt. Die besondere Vorabinformation und das Widerspruchsrecht bei Unterauftragsverarbeitern nach § 7 bleiben bestehen. Eine Änderung einer Webseite allein schreibt eine frühere Zustimmung nicht um.

(4) Deutsches Recht, Gerichtsstand wie in den AGB (§ 38 ZPO analog, Bochum soweit Kaufmann).

Anlage A – Technische und organisatorische Maßnahmen (TOMs)

Diese Anlage ist Bestandteil der Fassung 2026-09-09-demo14 und ersetzt für diese Fassung den bisherigen Verweis auf ein separates TOM-Erstdokument. Die folgenden technischen Angaben beschreiben den überprüften Produktionsstand. Organisatorische Verpflichtungen werden als solche benannt. Nicht belegte Maßnahmen werden nicht als umgesetzt ausgewiesen.

A.1 Verantwortlichkeit und Zutritt

Der Auftragsverarbeiter betreibt keine eigenen Rechenzentren. Physischer Zutritt, Stromversorgung und Schutz der Rechenzentrumsinfrastruktur liegen bei den eingesetzten Hostinganbietern. Deren Nachweise sind von den Maßnahmen des Auftragsverarbeiters zu unterscheiden; Zertifizierungen eines Anbieters gelten nicht automatisch für Richaard.

Verantwortlicher Ansprechpartner für Betrieb, Weisungen und Datenschutzvorfälle ist Nikita Erochok unter kontakt@richaard.de. Vor Zugriff durch weitere Personen sind Vertraulichkeitsverpflichtung, erforderlicher Berechtigungsumfang und Entzug der Rechte bei Wegfall der Aufgabe zu dokumentieren. Eine abgeschlossene Mitarbeiterschulung oder eine externe Zertifizierung wird nicht behauptet.

A.2 Zugang und Anmeldung

- App-Zugang erfolgt mit E-Mail und Passwort über die selbst betriebene Software Better Auth; Passwörter werden als Hash gespeichert.
- Die E-Mail muss bestätigt sein. Ein gültiger, signierter Nachweis aus der Website kann die bereits erfolgte Bestätigung übernehmen. Der Produktionszugang ist zusätzlich auf bestätigte Demo-Leads begrenzt.
- Sitzungen werden serverseitig geprüft. Der Sitzungscookie ist unter HTTPS abgesichert; Abmeldung beendet die aktive Sitzung. Ein Wechsel zu einem anderen Konto während einer Registrierung muss

ausdrücklich erfolgen.

• Cloud-Zugänge und Dienstkonten sind von Kundenkonten getrennt. Die tatsächlich eingerichtete Mehrfaktorauthentifizierung und regelmäßige Kontrolle administrativer Berechtigungen müssen organisatorisch nachgewiesen werden; eine verpflichtende Mehrfaktorauthentifizierung für alle App-Konten ist derzeit nicht umgesetzt.

A.3 Mandanten- und Zugriffstrennung

• Die Mandantenkennung wird aus dem serverseitig verifizierten Anmeldetoken abgeleitet, nicht aus einer vom Browser vorgegebenen Kennung.

• Datenbankabfragen begrenzen den Zugriff auf den jeweiligen Mandanten. Für die geschützten Fachtabellen besteht zusätzlich PostgreSQL Row Level Security; der Anwendungspfad verwendet eine eingeschränkte Datenbankrolle ohne Umgehungsrecht. Schlägt der erforderliche Rollenwechsel fehl, wird die Abfrage abgebrochen.

• Die administrative Datenbankverbindung bleibt für notwendige Schema- und Auth-Verwaltung getrennt. Sie ist kein Kunden-Zugang und kein allgemeiner Ersatz für die eingeschränkte Rolle.

• Matching-Sitzungen und Ergebnisse werden dem authentifizierten Mandanten zugeordnet. Browserzustand kann diese Zuordnung nicht übersteuern. Dateien und Ergebnisse werden über geschützte Anwendungsfunktionen bereitgestellt.

• Das Backend ist durch Cloud-Run-IAM geschützt. Das Frontend authentifiziert seine Backend-Aufrufe zusätzlich mit einem Diensttoken und dem Nutzertoken. Direkter öffentlicher Backend-Zugriff ist nicht freigegeben.

A.4 Übertragung, Speicher und Geheimnisse

Browserkommunikation erfolgt über HTTPS. Der Cloudflare-App-Proxy leitet Anfragen an Cloud Run weiter und setzt für App-Antworten Cache-Control auf private/no-store. Dabei wird TLS an den beteiligten Diensten terminiert; Cloudflare kann durchgeleitete Inhalte verarbeiten. Es besteht keine Ende-zu-Ende-Verschlüsselung, die den Verarbeitungsdiensten den Zugriff auf notwendige Klartexte entzieht.

Die Produktionsverbindung zu Neon verwendet TLS. Der Zugriff auf Cloud-Dienste erfolgt mit Dienstkonten; Produktionsgeheimnisse werden in Google Secret Manager hinterlegt und den benötigten Diensten zugewiesen. Runtime-Dienstkonten verwenden die Cloud-Identität statt eigens erzeugter JSON-Schlüssel. Geheimnisse gehören nicht in das Quellcode-Repository.

Systemmails werden über Mailgun EU versandt. Beim SMTP-Versand der App ist TLS erforderlich, Öffnungs- und Klicktracking sind deaktiviert. Im vorgesehenen Systemmail-Flow werden keine Bewerberunterlagen oder Matching-Ergebnisse verschickt. Antworten erreichen kontakt@richaard.de über STRATO.

A.5 Eingaben, Dateiverarbeitung und Missbrauchsschutz

• Uploads prüfen Dateityp, Signatur und Größenlimits; große Inhalte werden mit begrenzten Leseabschnitten verarbeitet.

• PDF-Verarbeitung hat ein Seitenlimit, DOCX-Verarbeitung eine Grenze für entpackte Inhalte; Extraktionen sind zeitlich begrenzt.

• Downloads setzen einen serverseitig bestimmten Medientyp und verhindern MIME-Sniffing.

• Stellenimporte begrenzen Hosts und Antwortgrößen, prüfen Weiterleitungen erneut und sperren nicht öffentliche Zieladressen. Die Verbindung wird an die geprüfte öffentliche Adresse gebunden.

• Demo-Limits begrenzen Lebensläufe und Matching-Läufe je Konto. Credits werden beim Matching-Start atomar verbraucht.

Diese Maßnahmen ersetzen keinen vollständigen Schadsoftware-Scanner. Ein solcher Scanner oder eine vollständige Anonymisierung der hochgeladenen Unterlagen wird nicht als vorhandene Funktion zugesichert.

A.6 Nachvollziehbarkeit und Änderungen

Die App protokolliert Vertragsannahmen als zusätzliche Ereignisse mit Mandant, handelnder Person, Unternehmensangaben, Zeitpunkt, Dokumentversion und SHA-256-Prüfsumme. Eine neue Zustimmung ersetzt nicht die bisherigen Ereignisse. Ein älterer Fehler bei der Zuordnung von Texten und Prüfsummen wird nicht rückwirkend durch Änderung historischer Ereignisse korrigiert; für die neue Fassung werden die vollständigen Dokumentdateien einschließlich Anlagen geprüft.

Betriebs- und Fehlerprotokolle werden in Google Cloud Logging verarbeitet. Sie können Kennungen, Dateinamen und Fehlermeldungen enthalten; eine lückenlose Protokollierung jedes einzelnen Lesezugriffs wird nicht zugesichert. Bei Diagnose und Support sind Datenzugriffe und Protokollinhalte auf das Erforderliche zu

beschränken.

Quellcodeänderungen werden versioniert und vor Veröffentlichung mit automatisierten Tests geprüft. Die Prüfungen umfassen unter anderem Authentifizierung, Mandantentrennung und Vertragsversionen. Ein externer Penetrationstest oder eine Zertifizierung des Gesamtsystems ist damit nicht nachgewiesen.

A.7 Verfügbarkeit und Wiederherstellung

Die Anwendung nutzt verwaltete Cloud-Dienste und lässt sich auf einen vorherigen veröffentlichten Softwarestand zurücksetzen. Dieser Software-Rollback stellt keine gelöschten Daten wieder her. Die aktive Wiederherstellungsfunktion für gelöschte Originaldateien sowie die bekannten Protokollfristen stehen in Anlage D.

Die exakten Neon-Wiederherstellungsfenster, vollständige Backup-Rotation, ein dokumentierter Wiederherstellungstest und verbindliche Wiederanlauf- bzw. Datenverlustziele sind noch nicht nachgewiesen. Sie werden deshalb nicht als zugesicherte Eigenschaften des Trials angegeben. Kunden müssen ihre Originalunterlagen selbst vorhalten. Der Auftragsverarbeiter bleibt verpflichtet, ein dem Risiko angemessenes Sicherungs- und Wiederherstellungsverfahren festzulegen und zu überprüfen.

A.8 KI und Zweckbindung

Profilerstellung, Embeddings und Bewertung verwenden Gemini über Vertex AI. Nur für den jeweiligen Verarbeitungsschritt benötigte Daten sollen übermittelt werden. Kriterien sind vor dem eigentlichen Matching durch den Nutzer zu bestätigen. Ergebnisse und Begründungen dienen als Entscheidungshilfe und können fehlerhaft sein; eine inhaltliche menschliche Prüfung ist erforderlich.

Es erfolgt keine eigene Einstellungs- oder Absageentscheidung durch Richaard. Emotionserkennung und biometrische Kategorisierung werden nicht eingesetzt. Der Kunde darf menschliche Prüfung nicht durch bloßes ungeprüftes Übernehmen einer Rangliste ersetzen und muss die Anforderungen des Art. 22 DSGVO prüfen.

A.9 Prüfstand der organisatorischen Maßnahmen

Vor einer abschließenden Freigabe sind insbesondere die Vertragsnachweise mit Unterauftragsverarbeitern einschließlich Transfergrundlagen, administrative Mehrfaktorauthentifizierung und Berechtigungsprüfungen, Vertraulichkeitsverpflichtungen, Incident-Ablauf sowie vollständige Lösch- und Wiederherstellungsnachweise zu dokumentieren. Diese offenen Nachweise sind nicht gleichbedeutend mit dem Nachweis, dass entsprechende Schutzmaßnahmen fehlen; sie sind in dieser Fassung noch nicht bestätigt.

Anlage B – Dienstleister und Unterauftragsverarbeitung

B.1 Cloudflare – App-Proxy und Auslieferung

Anbieter: Cloudflare, Inc., USA; maßgeblich ist die im Kundenvertrag bezeichnete Cloudflare-Vertragsgesellschaft.

Aufgabe und Daten: Weiterleitung und Absicherung der Zugriffe auf app.richaard.de. Darüber laufen auch Uploads, Chat-Anfragen und Antworten der Anwendung; betroffen sein können Bewerberunterlagen, Eingaben, Matching-Ergebnisse, Cookies und Verbindungsdaten. Cloudflare ist deshalb auch für den App-Verkehr in der Unterauftragnehmerliste enthalten, nicht nur als Website- oder DNS-Dienst.

Verarbeitung: globales Cloudflare-Netzwerk; keine festgelegte EU-Jurisdiktion für diesen Proxy. App-Antworten werden vom Proxy als nicht cachebar gekennzeichnet. Das schließt notwendige Sicherheits- und Betriebsverarbeitung des Anbieters nicht aus.

Vertrags- und Transferinformationen: Cloudflare Data Processing Addendum und die dortigen Unterauftragnehmer-/Transferregelungen; tatsächliche Einbeziehung und anwendbare Garantien sind für das Kundenkonto zu dokumentieren. [Cloudflare-DPA](https://www.cloudflare.com/cloudflare-customer-dpa/).

B.2 Google Cloud – Betrieb, Dateien und KI

Anbieter: Google Cloud EMEA Limited, Irland, nach Googles regulärer Zuordnung für eine deutsche Rechnungsadresse. Abweichende individuelle Vertragszuordnungen sind anhand des Kontovertrags zu prüfen; Google LLC und weitere Unternehmen können in der Unterauftragskette beteiligt sein.

Aufgabe und Daten: Cloud Run betreibt Frontend und Backend; Cloud Storage hält Originaldateien; Secret Manager schützt Betriebsgeheimnisse; Cloud Logging verarbeitet Betriebs- und Sicherheitsprotokolle. Gemini über Vertex AI erstellt Profile, Embeddings, Kriterien und Bewertungen aus den hierfür benötigten Bewerber-, Stellen- und Chat-Inhalten.

Verarbeitung: Cloud Run und Cloud Storage in Belgien (europe-west1), KI-Konfiguration eu. Für die Protokoll-Buckets und weitere Plattform-/Supportdienste besteht keine einheitliche Zusicherung ausschließlich europäischer Verarbeitung. Cloud SQL ist im beschriebenen Produktionspfad nicht provisioniert und gehört nicht zum eingesetzten Datenbankdienst.

Vertrags- und Transferinformationen: Google Cloud Data Processing Addendum einschließlich Unterauftrags- und Transferregelungen. Die konkrete Einbeziehung ist zu dokumentieren. Für KI gelten außerdem die Einschränkungen zu Training und Missbrauchsprüfung aus § 1 Abs. 4. [Google-Vertragsgesellschaft](https://cloud.google.com/terms/google-entity), [Google-Cloud-DPA](https://cloud.google.com/terms/data-processing-addendum), [Google zur KI-Datenverarbeitung](https://docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention).

B.3 Neon – Datenbank

Anbieter: Neon, LLC / Databricks, Inc., USA. Die veröffentlichten Neon-Bedingungen vom 5. August 2026 nennen Databricks, Inc. als Vertragspartner und Neon, LLC als verbundenes Unternehmen. Der für das bestehende Konto geltende Vertrag ist damit abzugleichen.

Aufgabe und Daten: PostgreSQL mit strukturierten Bewerberprofilen, Embeddings, Stellen, Kriterien, Bewertungen, Rankings, Chat-Sitzungen und zugehörigen Kennungen. Konto- und Vertragsdaten liegen technisch ebenfalls dort, unterliegen hinsichtlich eigener Zwecke aber der Datenschutzerklärung.

Verarbeitung: Datenbankregion Frankfurt (eu-central-1). Betriebs-, Support- und weitere Unterauftragsverarbeitung kann außerhalb des EWR stattfinden. Eine pauschale EU-only-Zusage wird nicht erteilt.

Vertrags- und Transferinformationen: geltende Neon-Produktbedingungen in Verbindung mit den einbezogenen Databricks-Vertrags-/Datenschutzbedingungen und der Unterauftragnehmerliste. Kontospezifische Geltung und Nachweise sind zu dokumentieren. [Neon-Vertragsbedingungen](https://neon.com/platform-terms).

B.4 Weitere Systeme und ihre Abgrenzung

- **Cloudflare D1:** speichert Demo-Anfragen und getrennte Werbeeinwilligungen in Westeuropa; es ist nicht die Datenbank für Bewerberunterlagen. Diese eigene Kontakt- und Zugangsverwaltung ist in der Datenschutzerklärung beschrieben. Sie ist vom durch B.1 erfassten App-Proxy zu unterscheiden.
- **Mailgun / Sinch Email:** EU-API für Website-Mails, EU-SMTP für App-Bestätigungen und Passwort-Reset. Verarbeitet Empfänger, Inhalte der Systemmail und Zustellstatus; kein vorgesehener Versand von CVs oder Rankings. Der genaue Sinch-Email-Vertragspartner richtet sich nach dem Versandkonto. Diese eigene Kontokommunikation ist in der Datenschutzerklärung erfasst.
- **STRATO GmbH:** eingehende Postfächer und Domain-Dienste. Bewerberunterlagen sollen nicht per Support-Mail eingereicht werden. Soweit im Einzelfall Auftragsdaten für eine Supportleistung per Mail verarbeitet werden müssen, sind Umfang, Weisung und einschlägige Unterauftragsbedingungen vorab zu klären; die bloße Nennung erweitert keine Weisung zum CV-Versand.
- **Better Auth, Nodemailer, ADK und CopilotKit:** eingesetzte Softwarebibliotheken. Die selbst betriebene Nutzung begründet allein keinen separaten SaaS-Unterauftrag. Die tatsächlichen externen Verarbeitungsdienste ergeben sich aus B.1 bis B.3.
- **Dittofeed:** vorbereitet, in der Produktion nicht aktiviert. **Google Analytics, Google Ads und Google Tag Manager:** nicht Teil dieses Recruiting-Verarbeitungspfads und aktuell nicht im Anwendungscode eingebunden. Eine spätere Aktivierung erfordert eine gesonderte Prüfung; bei neuen Unteraufträgen gilt § 7.

Die Links in dieser Anlage dienen als Quellen- und Nachweisverweise. Eine spätere Änderung einer Anbieterseite ändert nicht automatisch den zwischen den Parteien vereinbarten Leistungsumfang. Neue oder ersetzte Unterauftragsverarbeiter sind nach § 7 anzukündigen; die Nennung eines Dienstes ersetzt nicht den Abschluss erforderlicher Datenschutzverträge.

Anlage C – Weisungen, Betroffenenrechte und Vorfälle

C.1 Umfang und Übermittlung von Weisungen

Zulässige Weisungen umfassen Upload und Speicherung rechtmäßig erhobener Unterlagen, Stellenimport, Profilerstellung, Kriterienbestätigung, Matching, Anzeige, Rückgabe, Berichtigung, Einschränkung und Löschung. Sie werden über die dafür vorgesehenen App-Funktionen oder durch die vertretungsberechtigte Kontaktperson an kontakt@richaard.de erteilt. Zusätzliche Weisungen sind nachvollziehbar mit Datum, Absender, betroffenen Daten und gewünschter Maßnahme zu dokumentieren.

Weisungen zur Offenlegung an Unberechtigte, zum Umgehen der Mandantentrennung oder zur Nutzung von Auftragsdaten für fremde Zwecke werden nicht ausgeführt. Bei Zweifeln an der Berechtigung wird die anfragende Person angemessen verifiziert; bei Zweifeln an der Rechtmäßigkeit gilt § 4.

C.2 Unterstützung

Anfragen betroffener Personen zu Auftragsdaten werden dem verantwortlichen Kunden unverzüglich zugeleitet. Ohne dessen Weisung wird eine betroffene Person nicht eigenständig inhaltlich beschieden, soweit keine gesetzliche Pflicht besteht. Der Auftragsverarbeiter unterstützt bei der Suche nach betroffenen Datensätzen, ihrer Auskunft, Berichtigung, Rückgabe, Einschränkung und Löschung einschließlich abgeleiteter Profile und Ergebnisse. Der Umfang darf nicht allein auf die noch vorhandene Originaldatei begrenzt werden.

Bei Datenschutz-Folgenabschätzungen und Konsultationen werden verfügbare Informationen zur Verarbeitung, zu Schutzmaßnahmen und zu Unterauftragsverhältnissen bereitgestellt. Eine DSFA des Kunden wird nicht durch die technische Beschreibung dieser Anlage ersetzt.

C.3 Vorfallverfahren

Bei Bekanntwerden eines Vorfalls werden Umfang und betroffene Mandanten ermittelt, erforderliche Eindämmungsmaßnahmen eingeleitet und relevante Nachweise geschützt. Die Information nach § 8 nennt, soweit bekannt, Art des Vorfalls, betroffene Kategorien und ungefähre Anzahl von Personen/Datensätzen, wahrscheinliche Folgen, ergriffene bzw. geplante Maßnahmen und einen erreichbaren Ansprechpartner. Fehlende Angaben werden schrittweise ergänzt; auf eine vollständige Untersuchung wird mit der Erstinformation nicht gewartet.

Zeitpunkt, Untersuchung, Weisungen und Maßnahmen sind zu dokumentieren. Ein bereits regelmäßig geübter Incident-Prozess oder ein rund um die Uhr besetzter Support wird in dieser Fassung nicht zugesichert.

Anlage D – Rückgabe, Löschung und Wiederherstellung

D.1 Demo-Laufzeit und Löschung

Für ab Einführung neu registrierte App-Konten läuft die Demo ab erfolgreicher Registrierung genau 14 × 24 Stunden. Logins, Uploads und Passwort-Resets verlängern diese Frist nicht. Das konkrete Ende wird in der App angezeigt. Bei Einführung vorhandene Konten sind vorerst ausdrücklich ausgenommen; für diese gilt die bisherige Vereinbarung bis zu einer gesondert angekündigten Umstellung.

Mit Ablauf endet der Zugang. Der tägliche Löschlauf um 03:00 UTC entfernt Demo-Daten und App-Konto regulär innerhalb von 24 Stunden nach Ablauf aus den aktiven Systemen. Erfasst sind Originaldateien, Profile, Embeddings, Stellen, Kriterien, Bewertungen, Ranglisten, Chats, Sitzungen und Einstellungen. Frühere rechtmäßige Löschweisungen bleiben möglich. Eine geprüfte Exportanfrage an kontakt@richaard.de kann die Löschung ausschließlich zur Rückgabe um höchstens sieben Tage verschieben; die Demo bleibt gesperrt. Der Löschtermin wird auf einen täglichen Lauf innerhalb dieser Obergrenze gelegt. Der Kunde fragt die Rückgabe rechtzeitig an; das Fehlen einer Export-Schaltfläche beschränkt seine Rechte nicht.

Originaldateien bleiben im vorgesehenen Betrieb bis zum individuellen Demo-Ende verfügbar. Frühere Ein-Tages-Löschungen werden nicht rückgängig gemacht. Nach Löschung hält die konfigurierte Wiederherstellungsfunktion von Google Cloud Storage Dateien noch sieben Tage vor. Datenbank-Sicherungen und Dienstleisterprotokolle haben gesonderte Fristen; die 24-Stunden-Frist ist keine Zusage ihrer sofortigen vollständigen Entfernung. Bereits erteilte Löschungen müssen vor der Wiederaufnahme nach einer Wiederherstellung erneut berücksichtigt werden.

D.2 Durchführung und Nachweis

Die Löschung erfolgt getrennt nach Datenbank, Dateispeicher, Authentifizierung und Website-Zugang. Fehlgeschlagene Schritte werden nachgeholt und überwacht; eine bloße Zugangssperre gilt nicht als abgeschlossene Löschung. Auch verwaiste Dateien und abgeleitete Daten sind zu erfassen. Laufende Verarbeitung darf gelöschte Daten nicht wieder anlegen. Exporte werden verschlüsselt bereitgestellt und spätestens zum dokumentierten Löschtermin entfernt.

D.3 Protokolle und Sicherungskopien

Google-Cloud-Standardprotokolle haben derzeit eine Aufbewahrung von 30 Tagen; bestimmte gesonderte Audit-Protokolle 400 Tage. Erforderliche Nachweise zu konkreten Sicherheitsvorfällen können gesondert gesichert werden. Daten in Sicherungen werden nur zur Wiederherstellung oder aufgrund gesetzlicher Pflichten genutzt und unterliegen weiter den Schutz- und Zweckbindungspflichten dieses AVV.

Für Neon-Wiederherstellungsfenster und sämtliche Cloudflare-/Mail-Anbieterprotokolle ist eine kontospezifische vollständige Fristenübersicht noch zu dokumentieren. Eine pauschale 30-Tage-Gesamtlöschung oder eine 90-Tage-Obergrenze für alle Backups wird deshalb nicht zugesichert. Der Auftragsverarbeiter muss verbleibende Fristen und technische Einschränkungen bei einer konkreten Löschweisung ermitteln und dem Kunden mitteilen; unbestimmte Fristen begründen keine unbeschränkte Aufbewahrung.

D.4 Vertragsnachweise

Minimale Vertrags- und Löschungsnachweise werden grundsätzlich bis zum Ende des dritten Kalenderjahres nach dem Jahr des Demo-Endes zweckbeschränkt aufbewahrt. Dies dient der begründeten Nachweisführung und Anspruchsabwehr; es ist keine pauschale gesetzliche Speicherpflicht. Konkrete Streitfälle werden gesondert dokumentiert. Nicht erforderliche IP-Adressen und Browserangaben werden bei der Archivierung entfernt.

Die Annahmenachweise dieses AVV betreffen die eigene Vertragsverwaltung des Anbieters und sind von Bewerberdaten zu trennen. Neue Versionen werden gesondert angenommen. Historische Ereignisse mit alter Version und damaliger Prüfsumme bleiben als damalige Aufzeichnung erhalten; eine fehlerhafte frühere Textzuordnung wird dadurch nicht nachträglich zu einem vollständigen Textnachweis. Einzelheiten zur eigenen Datenverarbeitung stehen in der Datenschutzerklärung.

Ende des AVV einschließlich Anlagen A bis D – Fassung 2026-09-09-demo14, juristisch ungeprüfter Entwurf.