RECHTLICHES · APP

Datenschutzerklärung der App

Fassung vom 28. September 2026

Diese Datenschutzerklärung gilt für die Recruiting-Anwendung **Richaard unter app.richaard.de**: Zugang und Konto, die Organisation deines Unternehmens, den Vertragsschluss in der App, die Verarbeitung von Bewerbungsunterlagen sowie unsere Kommunikation mit dir. Für den Besuch von richaard.de gilt die Datenschutzerklärung der Website.

Stand: 28. September 2026.

1. Verantwortlicher und Kontakt

Nikita Erochok, Einzelunternehmer
Feierabendweg 23, 44799 Bochum, Deutschland
Datenschutz: kontakt@richaard.de

Die Anbieterkennzeichnung findest du im Impressum. Für Datenschutzanfragen wende dich unmittelbar an den genannten Verantwortlichen.

Für Konten, Organisationen, Vertragsnachweise und unsere eigene Kommunikation ist Nikita Erochok Verantwortlicher. Für Bewerberdaten und Stellen, die ein Unternehmen in Richaard verarbeitet, bleibt dieses Unternehmen verantwortlich; Richaard verarbeitet sie in dessen Auftrag. Einzelheiten regelt der Auftragsverarbeitungsvertrag (AVV).

2. Betrieb, Hosting und Sicherheit

Die App läuft auf **Google Cloud Run** in Belgien (`europe-west1`). Hochgeladene Dateien liegen in **Google Cloud Storage** in derselben Region. Zugangsdaten für den technischen Betrieb werden mit **Google Secret Manager** verwaltet. **Cloud Logging** erfasst Betriebs-, Fehler- und Sicherheitsprotokolle. Neben Verbindungsdaten können diese Protokolle Kontokennungen, Dateinamen, Vorgangskennungen und Angaben zu fehlgeschlagenen Aktionen enthalten.

Anfragen an app.richaard.de laufen über **Cloudflare**, das die Zugriffe weiterleitet und absichert. Dabei werden IP-Adresse, Zugriffszeit, aufgerufene Adresse, Browser- und Betriebssystemangaben, Statuscodes und Sicherheitsereignisse verarbeitet. Die übertragenen Inhalte der App passieren diesen Dienst ebenfalls; App-Antworten werden nicht zwischengespeichert.

Anmeldung, Registrierung und Passwort-Zurücksetzen schützen wir mit **Cloudflare Turnstile** vor automatisierten Zugriffen. Turnstile prüft dafür technische Merkmale deines Browsers und deiner Verbindung, einschließlich der IP-Adresse, und liefert uns ein Prüfergebnis. Zusätzlich begrenzen wir die Zahl der Anmelde- und Rücksetzversuche.

Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b DSGVO, soweit die Verarbeitung zur Bereitstellung der App erforderlich ist, und Art. 6 Abs. 1 lit. f DSGVO für den sicheren Betrieb, die Fehlerbehebung und die Abwehr von Missbrauch. Unser berechtigtes Interesse besteht darin, die Verfügbarkeit des Dienstes und die Daten seiner Nutzer zu schützen.

3. Zugang, Konto und Organisation

Richaard wird von Unternehmen als **Organisation** genutzt. Ein Konto entsteht nur über eine Einladung für eine bestimmte E-Mail-Adresse oder wird von uns für die vom Unternehmen benannte Person eingerichtet. Einladungen versenden wir nicht per E-Mail; den Link übergibt die einladende Person oder wir selbst. Richten wir das Konto ein, legst du dein Passwort über einen persönlichen, einmal verwendbaren Link fest. Bei einer Registrierung über eine Einladung bestätigst du deine E-Mail-Adresse.

Für Registrierung und Anmeldung nutzen wir **Better Auth als selbst betriebene Software innerhalb unserer App**. Deine Anmeldedaten gehen dabei nicht an einen externen Anmeldedienst. Die Daten liegen in unserer PostgreSQL-Datenbank bei **Neon** in Frankfurt (`eu-central-1`).

Wir verarbeiten insbesondere:

- Name, E-Mail-Adresse und gegebenenfalls Firmenname;
- einen Passwort-Hash, den Bestätigungsstatus sowie Einladungs-, Bestätigungs- und Rücksetzvorgänge;
- Konto- und Sitzungskennungen, Gültigkeitszeiten sowie bei der Anmeldung anfallende IP- und Browserinformationen;
- Organisation, Rolle (Administrator oder Mitglied) und die Kennzeichnung als Vertragskontakt;
- Einstellungen, Einführungsfortschritt, ausgewählte Stellen und Chat-Sitzungen;
- Nutzungszähler, etwa für das tägliche Kontingent an Chat-Anfragen und die Matchings deiner Organisation;
- Protokolle zu Team-Änderungen, Einladungen, Löschungen und von uns vorgenommenen Kontoaktionen.

Mitglieder deiner Organisation sehen deinen Namen bei den von dir gestarteten Chats und Aktionen. Administratoren sehen zusätzlich Name, E-Mail-Adresse und Rolle der Mitglieder. Wer die Organisation verlässt, wird in bisherigen Verläufen als ehemaliges Mitglied angezeigt.

Diese Daten dienen der Kontoführung, der Zugriffskontrolle, der Zusammenarbeit im Team, der Bereitstellung der App und der Einhaltung der vereinbarten Kontingente. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO; bei Ansprechpartnern und Mitarbeitenden eines Unternehmenskunden sowie zur Abwehr von Missbrauch Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse ist die Bereitstellung des vom Unternehmen beauftragten Dienstes für seine Beschäftigten.

Ohne E-Mail-Adresse, Passwort und die als erforderlich gekennzeichneten Angaben kann das Konto nicht bereitgestellt werden. Richaard richtet sich an berufliche Nutzer und Unternehmen, nicht an Kinder. Zahlungsdaten werden in der App nicht erhoben.

4. Vertragsschluss und Nachweise

AGB und AVV schließt der Vertragskontakt deines Unternehmens in der App ab. Dabei speichern wir Unternehmensname und -anschrift, die Funktion der handelnden Person und ihre Bestätigung, für das Unternehmen handeln zu dürfen, außerdem Kontokennung, Zeitpunkt, Version und Prüfsumme der angenommenen Dokumente sowie IP-Adresse und Browserkennung. Weitere Mitglieder bestätigen persönlich, die Verträge zu kennen; dafür speichern wir dieselben Nachweisangaben ohne Unternehmensdaten.

Die Nachweise dienen dem Beleg der Vertragsvereinbarungen und der Abwehr von Ansprüchen. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b und f DSGVO sowie, soweit gesetzlich vorgeschrieben, Art. 6 Abs. 1 lit. c DSGVO.

5. E-Mails und Support

Bestätigungs- und Passwort-Reset-Mails der App versenden wir über **Mailgun / Sinch Email** mit den europäischen Versand-Endpunkten. Der Anbieter verarbeitet Empfänger- und Absenderadresse, Nachrichteninhalt, Versandzeitpunkt, technische Nachrichtenkennungen sowie Zustell- und Fehlermeldungen. Öffnungs- und Klick-Tracking sind deaktiviert. Bewerberunterlagen oder Matching-Ergebnisse werden nicht per E-Mail verschickt.

Die App sendet keine Werbung und fragt keine Werbeeinwilligung ab. Die vorbereitete Anbindung an die Software **Dittofeed** ist in der Produktion nicht aktiviert.

Die Postfach-Infrastruktur für eingehende Nachrichten an unsere Domain liegt bei **STRATO**. Wenn du uns kontaktierst, verarbeiten wir deine Kontaktdaten und Nachricht zur Bearbeitung deines Anliegens. Sende Bewerbungsunterlagen bitte nicht per E-Mail, sondern nutze die App. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b DSGVO für vertragsbezogene Anliegen und Art. 6 Abs. 1 lit. f DSGVO für sonstige geschäftliche Anfragen.

6. Bewerberdaten und KI-gestütztes Matching

Bei hochgeladenen Lebensläufen, Stelleninformationen und darauf bezogenen Chat-Inhalten ist das jeweilige Kundenunternehmen verantwortlich. Richaard verarbeitet diese Informationen ausschließlich im Auftrag. Dazu können Identifikations- und Kontaktdaten, Ausbildung, Berufserfahrung, Qualifikationen, Referenzen und andere in den Unterlagen enthaltene Angaben gehören. Bitte lade keine für das Recruiting unnötigen oder unzulässig erhobenen Daten hoch.

Die Verarbeitung umfasst Textextraktion und Profilerstellung, die Speicherung von Dokumenten und strukturierten Profilen, mathematische Suchrepräsentationen (Embeddings), Volltext- und Ähnlichkeitssuche sowie die Erstellung von Bewertungskriterien, Bewertungen, Begründungen und Ranglisten. Chat-Eingaben, daraus entstehende Ergebnisse und gespeicherte Matching-Verläufe stehen den Mitgliedern der Organisation gemeinsam zur Verfügung.

Für Profilerstellung, Embeddings, Kriterien und Bewertung verwenden wir **Google Gemini über Vertex AI** mit dem EU-Endpunkt. Dabei werden die für den jeweiligen Schritt benötigten Dokumentinhalte, Textauszüge, Kriterien und Chat-Eingaben an Google übermittelt; gescannte oder nicht auslesbare PDF-Dateien werden dafür vollständig übermittelt. Für laufende Chats speichert Vertex AI Kontextinhalte höchstens eine Stunde zwischen. Neon speichert unter anderem Profile, Embeddings, Stellen, Bewertungen und Chat-Sitzungen; Cloud Storage speichert die hochgeladenen Dateien.

Bewerberdaten werden weder von uns noch von Google zum Training oder zur Feinabstimmung von KI-Modellen verwendet. Für Sicherheits- und Missbrauchsprüfungen kann Google nach seinen Bedingungen eine vorübergehende Verarbeitung vornehmen. Weitere Informationen: Google zur Verarbeitung von KI-Daten.

Das Kundenunternehmen muss die Rechtsgrundlage für die Verarbeitung der Bewerberdaten bestimmen und die Bewerber informieren. Soweit besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO betroffen sind, ist zusätzlich eine einschlägige Ausnahme erforderlich. Ein gewöhnliches Bewerbungsfoto ist nicht allein deshalb ein biometrisches Datum zur eindeutigen Identifizierung.

Richaard trifft keine Einstellungs- oder Absageentscheidung. KI-Bewertungen können die Auswahl erheblich beeinflussen. Der Kunde muss die Ergebnisse inhaltlich prüfen, korrigieren können und die Vorgaben zu automatisierten Entscheidungen nach Art. 22 DSGVO beachten. Emotionserkennung und biometrische Kategorisierung werden nicht eingesetzt.

7. Eingesetzte Dienstleister und internationale Verarbeitung

Die Anbieter erhalten Daten, soweit sie für ihre jeweilige Aufgabe benötigt werden. Für Bewerberdaten sind die Unterauftragsverarbeiter zusätzlich im AVV aufgeführt.

Dienst	Aufgabe und betroffene Daten	Derzeitige Konfiguration
Cloudflare, Inc., USA	Weiterleitung und Absicherung von app.richaard.de, Turnstile bei Anmeldung und Registrierung; Verbindungsdaten und durchgeleitete Inhalte	Globales Netzwerk, ohne festgelegte EU-Jurisdiktion
Google Cloud	App-Betrieb, Dateispeicherung, Protokolle, Secret Manager; Konto-, Verbindungs- und Auftragsdaten	Cloud Run und Cloud Storage in Belgien; weitere Plattformdienste können abweichende Standorte haben
Google Gemini / Vertex AI	Profilerstellung, Embeddings, Kriterien und Matching; dafür benötigte Bewerber-, Stellen- und Chat-Inhalte	EU-Endpunkt
Neon, Teil von Databricks	PostgreSQL mit Konto-, Organisations-, Sitzungs-, Vertrags- und Recruiting-Daten	Datenbankregion Frankfurt
Mailgun / Sinch Email	Bestätigungs- und Passwort-Reset-Mails; Nachrichteninhalt und Zustellstatus	Europäische SMTP-Endpunkte
STRATO GmbH, Deutschland	Domain- und Postfachdienste, eingehende Kommunikation	STRATO-Mail-Infrastruktur

Die Nutzung einer EU-Region schließt Zugriffe oder Verarbeitungen außerhalb des EWR, etwa für Support, Betrieb oder Sicherheitszwecke, nicht für sämtliche Anbieter aus. Insbesondere bei US-Anbietern sind Übermittlungen in Drittländer möglich.

Für solche Übermittlungen sind die Voraussetzungen der Art. 44 ff. DSGVO einzuhalten, insbesondere ein anwendbarer Angemessenheitsbeschluss oder geeignete Garantien wie die EU-Standardvertragsklauseln. Eine Berufung auf das EU-US Data Privacy Framework setzt eine wirksame Zertifizierung des konkreten Empfängers für die betreffende Verarbeitung voraus. Informationen zu den einschlägigen Garantien kannst du beim Verantwortlichen anfordern.

Anbieterinformationen: Cloudflare-Datenschutzvereinbarung, Google Cloud-Datenschutzvereinbarung, Neon-Vertragsbedingungen, Mailgun-Datenschutzinformationen, STRATO-Datenschutzinformationen.

8. Cookies und Browser-Speicher

Die App verwendet nur Speicher, der für die von dir angeforderten Funktionen erforderlich ist. Analyse-, Werbe- oder Tracking-Dienste setzen wir in der App nicht ein. Rechtsgrundlage für unbedingt erforderliche Speicherungen und Zugriffe ist § 25 Abs. 2 Nr. 2 TDDDG; für die anschließende Verarbeitung personenbezogener Daten gelten die jeweils oben genannten Rechtsgrundlagen.

Speicher	Zweck	Dauer
Cookie `__Secure-better-auth.session_token`	Zuordnung deiner angemeldeten Sitzung	Bis zu 7 Tage; bei fortgesetzter Nutzung kann die Sitzung verlängert werden; Abmeldung beendet die aktive Sitzung
Sitzungsspeicher, etwa ausstehende E-Mail-Bestätigung, Matching-Start und Einführungsschritte	Fortsetzung der von dir gestarteten Vorgänge	Bis zur Erledigung, Entfernung durch die App oder zum Ende der Tab-Sitzung
Lokaler Speicher, etwa Kontokennung, ausgewählte Stelle, Recruiting-Modus, Farbschema und abgeschlossene Einführung	Wiederherstellung deines Arbeitszustands und deiner Einstellungen	Bis zum Überschreiben oder Löschen durch die App bzw. durch dich im Browser; einzelne Einträge werden bei Abmeldung entfernt

Du kannst Cookies und Browser-Speicher in den Einstellungen deines Browsers löschen. Dadurch kann eine erneute Anmeldung nötig werden oder eine gespeicherte Einstellung verloren gehen. Das Löschen des Browser-Speichers löscht nicht dein Konto oder serverseitig gespeicherte Unterlagen.

Schriften werden lokal mit der App ausgeliefert. Es findet kein gesonderter Abruf bei Google Fonts statt.

9. Speicherdauer und Löschung

Konto und Organisation: Kontodaten speichern wir, solange du Mitglied einer Organisation bist und der Vertrag mit deinem Unternehmen besteht. Eine Kontolöschung in der App gibt es derzeit nicht; wende dich dafür an kontakt@richaard.de oder an einen Administrator deiner Organisation. Entfernt dich ein Administrator aus der Organisation, endet dein Zugriff sofort. Nach Vertragsende sperren wir den Zugang der Organisation und löschen Konto- und Organisationsdaten, soweit keine Aufbewahrungsgründe bestehen.

Sitzungen, Einladungen und Links: Sitzungen enden spätestens nach sieben Tagen ohne Verlängerung. Einladungen und Links zum Festlegen des Passworts sind sieben Tage gültig; ein Passwort-Link verliert mit seiner Verwendung oder mit der Ausstellung eines neuen Links seine Gültigkeit.

Vertragsnachweise: Nachweise über angenommene Vertragsfassungen behalten wir grundsätzlich bis zum Ende des dritten Kalenderjahres nach dem Jahr des Vertragsendes zur Nachweisführung und Anspruchsabwehr. Nicht mehr erforderliche IP-Adressen und Browserangaben entfernen wir dabei. Konkrete Streitfälle und gesetzliche Sonderpflichten werden gesondert dokumentiert.

Bewerberdaten: Während der Vertragslaufzeit löscht die App Bewerberdaten nicht automatisch nach Fristen; sie bleiben gespeichert, bis das Unternehmen sie löscht oder eine Löschung anweist. Die Löschung eines Lebenslaufs entfernt Datei, Profil, Bewertungen, zugehörige Rankings, Chat-Sitzungen mit Bezug und Zwischenspeicher bei Vertex AI in der Regel innerhalb weniger Minuten; im Matching-Verlauf bleibt ein neutraler Platzhalter. Einzelheiten regelt Anlage D des AVV.

Protokolle und Sicherungen: Gelöschte Dateien hält Google Cloud Storage noch sieben Tage wiederherstellbar vor. Die Datenbank erlaubt eine Wiederherstellung innerhalb der letzten sechs Stunden. Google-Cloud-Standardprotokolle werden derzeit 30 Tage gespeichert, bestimmte gesonderte Audit-Protokolle 400 Tage. Zusätzliche Sicherungen vor technischen Umstellungen löschen wir nach deren Abschluss. Cloudflare- und Maildienst-Protokolle unterliegen den Fristen der Anbieter. Bereits erteilte Löschungen werden nach einer Wiederherstellung erneut berücksichtigt.

10. Deine Rechte

Unter den gesetzlichen Voraussetzungen hast du das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit (Art. 15 bis 20 DSGVO). Erteilte Einwilligungen kannst du mit Wirkung für die Zukunft widerrufen.

Widerspruch: Bei einer Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO kannst du aus Gründen, die sich aus deiner besonderen Situation ergeben, widersprechen.

Für Daten, für die Richaard verantwortlich ist, schreibe an kontakt@richaard.de. Für Bewerberdaten wende dich vorrangig an das Unternehmen, bei dem du dich beworben hast bzw. das deine Daten in Richaard verarbeitet. Wir unterstützen dieses Unternehmen bei der Bearbeitung deiner Rechte.

Du kannst dich bei einer Datenschutzaufsichtsbehörde beschweren. Für unseren Sitz in Bochum ist die **Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen** zuständig: Postfach 20 04 44, 40102 Düsseldorf, Telefon +49 211 38424-0, ldi.nrw.de. Du kannst dich auch an die Behörde an deinem gewöhnlichen Aufenthaltsort wenden.

11. Sicherheit und Änderungen

Wir verwenden verschlüsselte Verbindungen, Zugangskontrollen und eine Trennung der Organisationen und ihrer Daten. Die technischen und organisatorischen Maßnahmen bei Auftragsdaten regelt der AVV. Eine absolute Sicherheit kann kein Internetdienst gewährleisten.

Die aktuelle Fassung dieser Erklärung steht unter richaard.de/datenschutz-app. Bei wesentlichen Änderungen informieren wir bestehende Nutzer, soweit erforderlich, zusätzlich.