

Datenschutzhinweise der jobnext24 GmbH

Mitarbeiterdownload — öffentliche Fassung für Mitarbeitende und Interessierte

Stand: Juli 2026

Hinweis zur Veröffentlichung

Diese Fassung ist für den öffentlichen Downloadbereich der Website bestimmt und dient zugleich als datenschutzbezogene Informationsgrundlage für externe Mitarbeitende (Leiharbeitnehmer) und interne Mitarbeitende der jobnext24 GmbH.

Die rechtliche Verbindlichkeit datenschutzbezogener Verhaltenspflichten für Mitarbeitende wird über die separate interne Weisung Datenschutz hergestellt, die vor Ort ausgehändigt und auf dieses Dokument verweist.

Dieses Dokument enthält keine internen Audit-Checklisten, Vertragsunterlagen, Freigabevermerke oder sonstige nicht veröffentlichungsfähige Kontrollinformationen. Einwilligungen, soweit im Einzelfall erforderlich, werden gesondert eingeholt; notwendige Beschäftigten- und Abrechnungsverarbeitungen beruhen vorrangig auf Vertrag, Gesetz, Art. 6 DSGVO i. V. m. § 26 BDSG oder berechtigten Interessen.

Kurzfassung

Diese Datenschutzhinweise informieren nach Art. 13, 14 und 21 DSGVO über die Verarbeitung personenbezogener Daten durch die jobnext24 GmbH. Sie berücksichtigen die Besonderheiten der Personaldienstleistung und Arbeitnehmerüberlassung, insbesondere Bewerbermanagement, Personalverwaltung, Disposition, Lohnabrechnung, Kundenkommunikation, Vertrieb, Website-Dienste, Messenger-Kommunikation, Newsletter-Versand über Brevo, Workflow-Automatisierung mit Make sowie die kontrollierte Nutzung von KI-Systemen wie ChatGPT/OpenAI Enterprise und dem KI-Telefonassistenten fonio.ai. Entscheidungen über Bewerbung, Einstellung, Einsatz, Vergütung, Abmahnung, Kündigung oder vergleichbar erhebliche Personalentscheidungen werden nicht ausschließlich automatisiert getroffen.

1. Verantwortlicher und Datenschutzkontakt

Angabe	Inhalt
Verantwortlicher	jobnext24 GmbH
Vertreten durch	Andreas Fiege (Geschäftsführer)
Anschrift	An der Reitbahn 2, 21218 Seevetal
Telefon	04105 – 14 98 410
E-Mail (allgemein)	info@jobnext24.de
Handelsregister	HRB 208422, Amtsgericht Lüneburg

Angabe	Inhalt
Datenschutzkontakt	Andreas Fiege, jobnext24 GmbH – Datenschutz, An der Reitbahn 2, 21218 Seevetal, E-Mail: a.fiege@jobnext24.de, Betreff: Datenschutz

Hinweis zum Datenschutzbeauftragten (DSB)

Die jobnext24 GmbH prüft die Pflicht zur Bestellung eines betrieblichen oder externen Datenschutzbeauftragten nach Art. 37 DSGVO und § 38 BDSG. Aufgrund der umfangreichen Verarbeitung von Beschäftigten- und Gesundheitsdaten im Rahmen der Arbeitnehmerüberlassung ist eine entsprechende Bestellung vorgesehen.

Bis zur förmlichen Bestellung steht Herr Andreas Fiege als Datenschutzkontakt zur Verfügung. Anfragen zum Datenschutz und zur Ausübung von Betroffenenrechten richten Sie bitte unter dem Betreff Datenschutz an: a.fiege@jobnext24.de.

Sobald ein Datenschutzbeauftragter förmlich bestellt ist, werden diese Hinweise mit dessen Kontaktdaten aktualisiert.

Falls für einzelne Verarbeitungsvorgänge gesonderte Datenschutzhinweise, Einwilligungserklärungen oder Vertragsunterlagen gelten, gelten diese ergänzend.

2. Geltungsbereich dieser Datenschutzhinweise

Diese Hinweise gelten für personenbezogene Daten von Bewerberinnen und Bewerbern, Kandidatinnen und Kandidaten, externen Mitarbeitenden (Leiharbeitnehmern), internen Mitarbeitenden, ehemaligen Beschäftigten, Kunden, Ansprechpartnern bei Kunden und Interessenten, Lieferanten, Geschäftspartnern sowie Nutzerinnen und Nutzern unserer Website und Kommunikationskanäle einschließlich Newsletter-Abonnentinnen und -Abonnenten.

Die jobnext24 GmbH ist als Personaldienstleister und Arbeitgeber im Bereich der Arbeitnehmerüberlassung darauf angewiesen, personenbezogene Daten rechtmäßig, nachvollziehbar und zweckgebunden zu verarbeiten. Hierzu gehören insbesondere Recruiting, Matching, Bewerberkommunikation, Anlage und Pflege von Personalstammdaten, Einsatzplanung, Überlassungsdokumentation, Arbeitszeit- und Fehlzeiterfassung, Lohnabrechnung, gesetzliche Meldungen, Kundenbetreuung, Vertrieb, Website- und Marketingprozesse, Newsletter-Versand, Workflow-Automatisierung und interne Organisation.

Diese Informationen gelten unabhängig davon, ob die Daten über unsere Website, E-Mail, Telefon, den KI-Telefonassistenten (fonio.ai), persönliche Gespräche, Messenger-Dienste, Bewerbungsportale, zvoove-Systeme, Kundenunternehmen, öffentlich zugängliche Quellen, Make-Automatisierungen oder sonstige berechtigte Quellen erhoben werden.

3. Datenschutzgrundsätze

Wir verarbeiten personenbezogene Daten nach den Grundsätzen der Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Innerhalb unseres Unternehmens erhalten nur die Personen Zugriff auf Daten, die diese für ihre Aufgaben benötigen. Daten werden nicht für Zwecke verwendet, die mit dem ursprünglichen Zweck unvereinbar sind, es sei denn, eine gesetzliche Grundlage, eine wirksame Einwilligung oder ein überwiegendes berechtigtes Interesse lässt dies zu.

- Keine Verarbeitung ohne Zweck und Rechtsgrundlage.
- Keine Nutzung privater KI- oder Messenger-Accounts für personenbezogene Geschäftsdaten.
- Keine ausschließlich automatisierten Personalentscheidungen.
- Besondere Kategorien personenbezogener Daten werden nur verarbeitet, wenn dies arbeits-, sozialversicherungs-, tarif-, gesundheits- oder arbeitsschutzrechtlich erforderlich ist oder eine ausdrückliche Einwilligung vorliegt.
- Personenbezogene Daten werden gelöscht oder gesperrt, sobald der Zweck entfällt und keine gesetzlichen Aufbewahrungs-, Nachweis- oder Verteidigungspflichten entgegenstehen.

4. Betroffene Personengruppen und typische Datenkategorien

Personengruppe	Typische Datenkategorien
Bewerber / Kandidaten	Name, Kontaktdaten, Lebenslauf, Zeugnisse, Qualifikationen, Berufserfahrung, Sprachkenntnisse, Führerschein, Mobilität, Verfügbarkeit, Gehalts- und Einsatzwünsche, Interviewnotizen, Eignungseinschätzungen, Kommunikationsverlauf, Einwilligungen, Absage- und Statusinformationen.
Externe Mitarbeitende / Leiharbeitnehmer	Stammdaten, Kontaktdaten, Geburtsdaten, Sozialversicherungs- und Steuerdaten, Bankverbindung, Vertragsdaten, Einsatzdaten, Arbeitszeiten, Fehlzeiten, Urlaubs- und Arbeitszeitkonten, Qualifikationen, Arbeitsschutzunterweisungen, Arbeitserlaubnisse, Aufenthaltsstatus, Lohn- und Abrechnungsdaten, Bescheinigungen, Korrespondenz, Personalnotizen, Anrufmetadaten und transkribierte Anliegen bei Nutzung des KI-Telefonassistenten.
Interne Mitarbeitende	Personalstamm, Bewerbungs- und Vertragsdaten, Arbeitszeit, Urlaub, Fehlzeiten, Lohn und Gehalt, Rollen und Berechtigungen, Leistungs- und Gesprächsdokumentation, IT-Nutzungsdaten, Schulungsnachweise, Kommunikationsdaten, Anrufmetadaten und transkribierte Anliegen bei Nutzung des KI-Telefonassistenten.
Kunden, Interessenten, Ansprechpartner	Name, Funktion, dienstliche Kontaktdaten, Arbeitgeber/Unternehmen, Kommunikationsverlauf, Vakanzen, Anforderungsprofile, Einsatzorte, Konditionen, Abrechnungsdaten, Feedback, Vertrags- und Auftragsdaten.

Personengruppe	Typische Datenkategorien
Lieferanten / Dienstleister	Kontakt- und Vertragsdaten, Zahlungsdaten, Leistungsnachweise, Kommunikationsdaten, Berechtigungs- und Supportdaten.
Newsletter-Abonnenten	Vorname, Nachname, E-Mail-Adresse, Einwilligungsdatum und -nachweis (Double-Opt-in), Öffnungs- und Klickdaten (sofern Tracking aktiviert).
Website-Nutzer	IP-Adresse, Logdaten, Browser-/Gerätedaten, Zeitpunkt des Zugriffs, aufgerufene Seiten, Kontaktformularinhalte, Cookie- und Einwilligungsinformationen, Tracking-Pixel-Ereignisse (Meta-Pixel/CAPI), Conversion-Ereignisse.

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO können im Beschäftigungs- und Einsatzkontext insbesondere Gesundheitsdaten (z. B. Arbeitsunfähigkeit ohne Diagnose, Arbeitsunfall, Arbeitsschutz, Vorsorgeuntersuchung), Angaben zur Schwerbehinderung, Religionszugehörigkeit im Rahmen der Lohnsteuer, Gewerkschafts- oder Tarifbezug, Mutterschutz-/Elternzeitdaten oder vergleichbare besonders schützenswerte Informationen sein. Diagnosen werden grundsätzlich nicht aktiv angefordert; sollten solche Informationen eingehen, werden sie nur verarbeitet, soweit dies rechtlich erforderlich ist, andernfalls gelöscht oder auf das notwendige Minimum reduziert.

5. Herkunft der Daten

Wir erhalten personenbezogene Daten insbesondere von den betroffenen Personen selbst, aus Bewerbungsunterlagen, Gesprächen, E-Mails, Telefonaten (einschließlich Anrufen an den KI-Telefonassistenten), Messenger-Nachrichten, Bewerbungsportalen, Kundenanforderungen, Kundenunternehmen, öffentlich zugänglichen beruflichen Quellen, Stellenanzeigen, Social-Media-/Business-Netzwerken, der Bundesagentur für Arbeit, Sozialversicherungsträgern, Krankenkassen, Finanzbehörden, Gerichten, Rechtsanwälten, Steuerberatern, Berufsgenossenschaften und anderen berechtigten Stellen.

Bei Active Sourcing und Vertrieb können berufsbezogene Kontaktdaten und Informationen aus öffentlich zugänglichen Quellen oder aus professionellen Datenbanken (z. B. Index Anzeigendaten / IndexMedia) verarbeitet werden. Dies erfolgt nur, soweit ein berechtigtes Interesse besteht und die schutzwürdigen Interessen der betroffenen Personen nicht überwiegen.

Informationspflicht bei Datenerhebung aus Drittquellen: Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben (z. B. bei Active Sourcing), informieren wir die betroffene Person gemäß Art. 14 DSGVO über die Verarbeitung, in der Regel innerhalb eines Monats nach Erhebung, spätestens jedoch bei der ersten Kontaktaufnahme. Auf Wunsch wird die Verarbeitung sofort eingestellt.

6. Zwecke und Rechtsgrundlagen der Verarbeitung

Die nachfolgende Übersicht beschreibt die wesentlichen Verarbeitungsvorgänge. Je nach Einzelfall können mehrere Rechtsgrundlagen gleichzeitig einschlägig sein. Bei Beschäftigtendaten gilt § 26 BDSG i. V. m. Art. 6 DSGVO; unter Berücksichtigung der EuGH-Rechtsprechung (Urteil C-34/21) wird primär auf Art. 6 DSGVO abgestellt.

Verarbeitung	Zweck	Rechtsgrundlage
Bewerbung, Recruiting, Auswahl	Durchführung des Bewerbungsverfahrens, Prüfung von Qualifikation und Eignung, Terminabstimmung, Kommunikation, Dokumentation.	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 Abs. 1 BDSG; bei freiwilligen Angaben Art. 6 Abs. 1 lit. a DSGVO.
Bewerberpool / längere Speicherung	Speicherung für spätere passende Einsätze oder Vermittlungen.	Art. 6 Abs. 1 lit. a DSGVO (Einwilligung); Widerruf jederzeit möglich.
Active Sourcing und Kandidatenansprache	Ansprache geeigneter Personen über berufliche Netzwerke, öffentliche Profile, Empfehlungen oder berufsbezogene Datenbanken.	Art. 6 Abs. 1 lit. f DSGVO; Informationspflicht nach Art. 14 DSGVO.
Kandidatenprofile / Vorstellung bei Kunden	Erstellung und Übermittlung passender Profile zur Besetzung von Vakanzen und Einsätzen.	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG; ggf. Art. 6 Abs. 1 lit. a DSGVO.
Personalverwaltung / Beschäftigung	Begründung, Durchführung und Beendigung von Arbeitsverhältnissen, Personalakte, Vertragsverwaltung, Bescheinigungen, Mitarbeitergespräche.	Art. 6 Abs. 1 lit. b, c DSGVO i. V. m. § 26 Abs. 1 BDSG.
Arbeitnehmerüberlassung / AÜG	Einsatzplanung, Überlassungsdokumentation, Equal Pay, Höchstüberlassungsdauer, Nachweise gegenüber Kunden und Behörden.	Art. 6 Abs. 1 lit. b, c DSGVO i. V. m. § 26 BDSG; AÜG.
Arbeitszeit, Fehlzeiten, Urlaub, Disposition	Planung, Einsatzsteuerung, Abrechnung, Nachweis, Kontrolle von Ruhezeiten und Fehlzeiten.	Art. 6 Abs. 1 lit. b, c DSGVO i. V. m. § 26 BDSG; Art. 9 Abs. 2 lit. b DSGVO bei Gesundheitsdaten.
Lohnabrechnung, Steuern, Sozialversicherung	Entgeltabrechnung, ELStAM, DEÜV, Krankenkassenmeldungen, Berufsgenossenschaft, EEL, Zahlungen, Pfändungen, Bescheinigungen.	Art. 6 Abs. 1 lit. b, c DSGVO; § 26 BDSG; Art. 9 Abs. 2 lit. b DSGVO.

Verarbeitung	Zweck	Rechtsgrundlage
Kundenverwaltung, Aufträge, Faktura	Vertragsanbahnung, Auftragserfassung, Abrechnung, Forderungsmanagement.	Art. 6 Abs. 1 lit. b, c, f DSGVO.
Vertrieb und Leadgewinnung	B2B-Ansprache, Pflege von Interessenten- und Ansprechpartnerdaten.	Art. 6 Abs. 1 lit. f DSGVO; § 7 UWG bei elektronischer Werbung.
Newsletter-Versand (Brevo)	Versand von Informations- und Werbe-E-Mails an Abonnenten.	Art. 6 Abs. 1 lit. a DSGVO (Double-Opt-in); Widerruf jederzeit.
Messenger-/SuperChat-/WhatsApp-Kommunikation	Schnelle Abstimmung zu Disposition, Erreichbarkeit, Kundenkommunikation; teilweise KI-gestützte Antwortvorschläge mit menschlicher Freigabe vor Versand (siehe Ziffer 10.6).	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG; Art. 6 Abs. 1 lit. f DSGVO.
Website-Analyse (Google Analytics 4)	Auswertung Nutzerverhalten, Reichweitenmessung.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG (Einwilligung).
Werbung / Tracking (Google Ads, Meta-Pixel/CAPI/Custom Audiences)	Conversion-Messung, Remarketing, Zielgruppen-Targeting.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG (Einwilligung); für Meta-Pixel zusätzlich Art. 26 DSGVO (gemeinsame Verantwortlichkeit).
KI-Unterstützung (ChatGPT Enterprise)	Erstellung und Verbesserung von Texten, Recherche, Strukturierung.	Art. 6 Abs. 1 lit. f DSGVO; Art. 6 Abs. 1 lit. b/c DSGVO soweit erforderlich.
KI-Telefonassistent (fonio.ai)	Telefonische Bearbeitung von Anliegen der Mitarbeitenden; anfänglich außerhalb der Bürozeiten, schrittweise Erweiterung auf allgemeine Mitarbeiteranliegen (z. B. Krankmeldungen, Verfügbarkeit, Einsatz, Urlaub). Bewerber und Kunden werden derzeit nicht bearbeitet.	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG (Beschäftigungsverhältnis); ergänzend Art. 6 Abs. 1 lit. f DSGVO.
Workflow-Automatisierung (Make)	Verknüpfung und Synchronisation interner Prozesse zwischen freigegebenen Systemen.	Art. 6 Abs. 1 lit. f DSGVO; bei Bewerber-/Beschäftigtendaten zusätzlich Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG.
IT-Sicherheit, Protokolle	Schutz der Systeme, Zugriffssteuerung, Nachvollziehbarkeit, Backups.	Art. 6 Abs. 1 lit. c, f DSGVO; Art. 32 DSGVO.
Rechtsdurchsetzung und Verteidigung	Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche.	Art. 6 Abs. 1 lit. f DSGVO; Art. 9 Abs. 2 lit. f DSGVO.

7. Besondere Hinweise zur Zeitarbeit und Arbeitnehmerüberlassung

Als Personaldienstleister verarbeitet jobnext24 Daten in einem Dreiecksverhältnis zwischen Bewerber bzw. Mitarbeiter, jobnext24 als Arbeitgeber bzw. Verantwortlichem und dem Kundenunternehmen als Entleiher bzw. Auftraggeber. Hieraus ergeben sich besondere Transparenz- und Nachweispflichten.

7.1 Bewerbermanagement, Matching und Kandidatenprofile

Wir verarbeiten Bewerberdaten, um passende Beschäftigungsmöglichkeiten und Einsätze zu prüfen. Hierzu können Such-, Filter- und Matchingfunktionen verwendet werden. Matching bedeutet, dass Daten wie Beruf, Qualifikation, Erfahrung, Verfügbarkeit, Mobilität, Arbeitszeitwunsch, Entgeltgruppe, Einsatzort und Kundenanforderung miteinander abgeglichen werden. Das Ergebnis ist eine Entscheidungshilfe für unsere Mitarbeitenden, aber keine eigenständige Entscheidung des Systems.

- Eine Absage, Einladung, Einstellung, Einsatzzuweisung oder Profilübermittlung erfolgt nicht ausschließlich automatisiert.
- Kandidatenprofile werden auf das erforderliche Maß beschränkt. Sensible Angaben werden nur übermittelt, wenn sie für den konkreten Einsatz erforderlich und rechtlich zulässig sind.
- Fotos, Videos und besonders persönliche Zusatzangaben werden nur verarbeitet, wenn eine wirksame Einwilligung vorliegt.
- Bei Profilvertrieb und Kandidatenvorstellung wird vorab geprüft, ob eine Anonymisierung oder Pseudonymisierung ausreicht oder ob eine namentliche Übermittlung erforderlich ist.
- Betroffene können jederzeit eine Erläuterung des Matching-Ergebnisses anfragen.

7.2 Externe Mitarbeitende, Einsatzplanung und Kundenübermittlung

Zur Durchführung der Arbeitnehmerüberlassung verarbeiten wir Daten über Einsatzort, Tätigkeit, Qualifikation, Einsatzbeginn, Einsatzende, Arbeitszeiten, Schichten, Arbeitsschutzanforderungen, Kundenanforderungen, Entgeltgruppe, Branchenzuschläge, Equal Pay, Höchstüberlassungsdauer und sonstige einsatzbezogene Informationen. Kundenunternehmen erhalten nur die Daten, die sie für die Durchführung des Einsatzes, Arbeitsschutz, Zugang, Einsatzkoordination, Leistungsnachweis, Abrechnung und gesetzliche Pflichten benötigen.

Gemeinsame Verantwortlichkeit (Art. 26 DSGVO): Soweit jobnext24 und ein Kundenunternehmen im Einzelfall gemeinsam über Zwecke und Mittel der Datenverarbeitung entscheiden (z. B. bei Zeiterfassung beim Kunden, Zugangskontrollen oder Einsatzdokumentation), können sie gemeinsame Verantwortliche im Sinne von Art. 26

DSGVO sein. In diesem Fall wird eine entsprechende Vereinbarung geschlossen. Betroffene können den wesentlichen Inhalt auf Anfrage erhalten.

7.3 Arbeitszeit, Fehlzeiten, Gesundheit und Arbeitsschutz

Arbeitszeiten, Fehlzeiten, Urlaub, Arbeitsunfähigkeit, Arbeitsunfälle und arbeitsschutzrelevante Informationen werden verarbeitet, soweit dies für Einsatzplanung, Lohnabrechnung, Entgeltfortzahlung, Arbeitsschutz, Berufsgenossenschaft, gesetzliche Meldungen oder die Durchführung des Arbeitsverhältnisses erforderlich ist. Diagnosen werden nicht benötigt und sollen nicht übermittelt werden. Bei Arbeitsunfällen können Angaben zum Unfallhergang und zur Verletzung verarbeitet werden, soweit dies für gesetzliche Melde- und Nachweispflichten erforderlich ist.

7.4 Aufenthalts- und Arbeitserlaubnis, Identitäts- und Berechtigungsprüfungen

Soweit gesetzlich erforderlich, verarbeiten wir Angaben und Nachweise zu Identität, Aufenthaltsstatus, Arbeitserlaubnis, Sozialversicherung, Steuermerkmalen, Führerschein, Qualifikation, Schulungen, Sicherheitsunterweisungen, Vorsorgeuntersuchungen und sonstigen Einsatzvoraussetzungen. Diese Daten dienen der rechtssicheren Beschäftigung, der Vermeidung unerlaubter Beschäftigung und der Erfüllung arbeits-, sozialversicherungs-, steuer-, arbeitsschutz- und AÜG-bezogener Pflichten.

7.5 Lohnabrechnung und gesetzliche Meldungen

Für die Lohnabrechnung verarbeiten wir abrechnungsrelevante Stamm- und Bewegungsdaten, Arbeitszeiten, Zuschläge, Fehlzeiten, Bankdaten, Steuerdaten, Sozialversicherungsdaten, Krankenkassendaten, Pfändungen, Darlehen, Abschläge, Urlaub, Arbeitszeitkonten, Bescheinigungen und gesetzliche Meldungen. Daten können an Sozialversicherungsträger, Krankenkassen, Finanzverwaltung, Berufsgenossenschaften, Banken, Steuerberater, Lohnabrechnungsdienstleister und Behörden übermittelt werden.

8. Website, Cookies, Analyse, Werbung und Online-Kommunikation

Diese Ziffer konsolidiert die Informationen zur Online-Datenverarbeitung. Die konkrete Aktivierung einzelner Analyse-, Marketing- oder Drittanbieterdienste richtet sich nach der technischen Konfiguration der Website und, soweit erforderlich, nach der Einwilligung über das eingesetzte Consent-Tool.

Dienst	Daten	Zweck	Rechtsgrundlage
Webhosting (IONOS SE)	Beim Aufruf der Website können Browsertyp/-version, Betriebssystem, Referrer-URL, Hostname bzw. IP-	Bereitstellung, Stabilität, Fehleranalyse und Sicherheit der Website.	Art. 6 Abs. 1 lit. f DSGVO; AVV nach Art. 28 DSGVO; Server in Deutschland.

Dienst	Daten	Zweck	Rechtsgrundlage
	Adresse, Uhrzeit der Serveranfrage und aufgerufene Seiten verarbeitet werden. Anbieter: IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland.		
Cookies und Consent-Tool	Technisch erforderliche Cookies sowie, nach Einwilligung, Analyse-/Marketing-Cookies.	Bereitstellung der Website, Einwilligungsverwaltung, Reichweitenmessung, Marketing.	Art. 6 Abs. 1 lit. f DSGVO bzw. § 25 Abs. 2 Nr. 2 TDDDG für technisch Erforderliches; Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG für nicht erforderliche Cookies.
Kontaktformular / Online-Bewerbungen (zvoove Cockpit)	Eingegebene Daten wie Name, E-Mail-Adresse, Nachricht, Bewerbungsunterlagen. Anbieter: zvoove GmbH, Thaliastraße 7, 90443 Nürnberg.	Bearbeitung von Anfragen und Bewerbungen.	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 Abs. 1 BDSG (Bewerbung); Art. 6 Abs. 1 lit. f DSGVO (Kontakt); AVV mit zvoove.
Google Tag Manager	Container-ID GTM-WW2RR66P; technische Verwaltung von Tags. Eigene Datenerhebung nur in geringem Umfang.	Zentrale Verwaltung der Marketing-/Analyse-Tags.	Art. 6 Abs. 1 lit. f DSGVO für Einbindung; nachgelagerte Dienste nur nach Einwilligung.
Google Analytics 4 / Google-Signale	Nutzungsdaten, Geräte-/Browserdaten, Seitenaufrufe, Verweildauer, IP-Anonymisierung; bei Google-Signalen zusätzlich demografische Daten.	Reichweitenmessung, Verbesserung der Website.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG; Google Ireland Limited; SCC + DPF (Participant 5780).
Google Ads (Conversion, Remarketing, Kundenabgleich)	Cookie-/Gerätekennungen, Klick- und Conversion-Daten, gehashte Kundenlisten.	Werbeschaltung, Conversion-Messung, Remarketing.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG; SCC + DPF.
Meta-Pixel / Conversion API / Custom Audiences	Pixel-Ereignisse, IP, User-Agent, ggf. gehashte Kontakte. Anbieter: Meta Platforms Ireland Limited.	Kampagnenmessung, Zielgruppenbildung, Remarketing.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG; gemeinsame Verantwortlichkeit nach Art. 26 DSGVO; SCC + DPF (Participant 4452).
Adobe Fonts	Bei externer Einbindung IP-Adresse	Einheitliche Darstellung von Schriftarten.	Art. 6 Abs. 1 lit. f DSGVO bei lokaler Einbindung; Art.

Dienst	Daten	Zweck	Rechtsgrundlage
	und Zugriffsdaten an Adobe. Anbieter: Adobe Systems Incorporated, USA.		6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG bei externer Einbindung; SCC + DPF (Participant 5660).
OpenStreetMap	IP-Adresse, Browser-/Gerätedaten, Karteninteraktionen. Anbieter: OpenStreetMap Foundation, Cambridge, UK.	Darstellung von Standorten.	Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 25 Abs. 1 TDDDG; UK – Angemessenheitsbeschluss.
Newsletter (Brevo)	Vorname, Nachname, E-Mail, Einwilligungsnachweis (Double-Opt-in), Öffnungs-/Klickdaten. Anbieter: Brevo GmbH, Tochter der Sendinblue SAS, 17 rue de Salneuve, 75017 Paris, Frankreich.	Versand und Verwaltung von Newslettern.	Art. 6 Abs. 1 lit. a DSGVO (Einwilligung); AVV; bei Subauftragnehmern in Drittländern: SCC.
WhatsApp Business / SuperChat	Telefonnummer, Profilname, Nachrichteninhalte, Zeitpunkte, Metadaten. Anbieter WhatsApp: WhatsApp Ireland Limited. SuperChat: Superchat GmbH, Berlin.	Schnelle Kommunikation.	Art. 6 Abs. 1 lit. b/f DSGVO; ggf. Einwilligung. SCC + DPF (Participant 7735 für WhatsApp).

9. Eingesetzte Systeme und Softwarelösungen

Die nachfolgende Übersicht beschreibt die von uns eingesetzten Kernsysteme. Die konkrete Konfiguration, Rollen- und Rechtevergabe sowie Protokollierung werden intern dokumentiert und regelmäßig überprüft.

System	Zweck	Datenarten	Datenschutzanforderung
zvoove Cockpit / PDL / One / Payroll / Work App	Bewerbermanagement, Personalverwaltung, Disposition, Auftragsverwaltung, Lohnabrechnung, mobile App für Mitarbeitende.	Bewerber-, Personal-, Kunden-, Einsatz-, Arbeitszeit-, Abrechnungsdaten.	AVV nach Art. 28 DSGVO; Verarbeitung innerhalb EU; Rollen- und Rechtekonzept.
SuperChat	Multichannel-Kommunikation (E-Mail, SMS, WhatsApp Business).	Kontaktdaten, Nachrichteninhalte, Metadaten.	Superchat GmbH, Berlin; AVV; keine sensiblen Daten über Messenger.

System	Zweck	Datenarten	Datenschutzanforderung
WhatsApp Business	Direkte Kommunikation mit Bewerbern/Kunden/Mitarbeitenden.	Kontaktdaten, Nachrichteninhalte, Metadaten.	WhatsApp Ireland Limited; AVV; SCC + DPF (Participant 7735); kein Adressbuchabgleich.
Brevo (Newsletter)	Versand und Verwaltung von E-Mail-Newslettern.	Vorname, Nachname, E-Mail, Einwilligungsnachweis.	Brevo GmbH, Tochter Sendinblue SAS (Frankreich, EU); AVV; SCC für Subauftragnehmer.
ChatGPT / OpenAI Enterprise	Texterstellung, Recherche, Strukturierung.	Möglichst anonymisierte Sachverhalte; nur in Enterprise-Umgebung.	DPA/AVV mit OpenAI; EU-U.S. Data Privacy Framework; kein Training mit Eingaben.
fonio.ai (KI-Telefonassistent)	Telefonische Bearbeitung von Anliegen der Mitarbeitenden; anfänglich außerhalb der Bürozeiten, schrittweise Erweiterung auf allgemeine Mitarbeiteranliegen.	Telefonnummer, Zeitpunkt, transkribierte Anliegen. KEINE dauerhafte Audio-Speicherung – nur Live-Transkription der Sprache in Text.	fonio GmbH, Deutschland; AVV nach Art. 28 DSGVO; Verarbeitung innerhalb EU; Ansagepflicht nach Art. 50 KI-VO.
IndexMedia / Index Anzeigendaten	Vertriebliche Recherche, Vakanzen, Leadgenerierung.	Unternehmensdaten, dienstliche Ansprechpartner.	Berechtigtes Interesse; UWG bei Werbung.
IONOS (Webhosting)	Betrieb der Website jobnext24.de.	IP-Adressen, Server-Logfiles.	AVV mit IONOS SE; Server in Deutschland.
Google Tag Manager, Analytics 4, Ads	Verwaltung von Tags, Webanalyse, Werbung.	Cookies, Nutzungs-/Conversion-Daten.	Google Ireland Limited; SCC + DPF (Participant 5780); Einwilligung.
Meta-Pixel / CAPI / Custom Audiences	Werbe-Targeting bei Facebook/Instagram.	Pixel-Ereignisse, gehashte Kontakte.	Meta Platforms Ireland Limited; Art. 26 DSGVO; SCC + DPF (Participant 4452).
Adobe Fonts, OpenStreetMap	Schriftarten und Karten auf der Website.	IP-Adresse, Nutzungsdaten.	SCC + DPF bzw. Angemessenheitsbeschluss UK.
Make (Make.com)	Workflow-Automatisierung, interne Prozessverknüpfung.	Je nach Workflow; aktuell keine Bewerberdaten.	Make s.r.o., Prag, Tschechien (EU); AVV; kein Drittlandtransfer.
Cookie-Consent-Tool	Einwilligungs-Verwaltung.	Consent-ID, Status, Zeitpunkt.	§ 25 Abs. 2 Nr. 2 TDDDg; AVV.
Office, E-Mail, Dateiablage, Backups	Allgemeine Kommunikation und Dokumentation.	Bewerber-, Mitarbeiter-, Kunden-, Kommunikationsdaten.	Zugriffsrechte, Verschlüsselung, Löschkonzept.

10. Einsatz von Künstlicher Intelligenz (KI)

Wir setzen KI-Systeme nur kontrolliert, zweckgebunden und unter menschlicher Verantwortung ein. KI dient der Unterstützung, nicht dem Ersatz menschlicher Personal- oder Geschäftsentscheidungen. Dies gilt insbesondere für ChatGPT/OpenAI, den KI-Telefonassistenten fonio.ai sowie für KI-Funktionen in eingesetzten Fachsystemen wie zvoove Cockpit oder Automatisierungsszenarien mit Make.

10.1 Zulässige KI-Nutzung

- Entwurf, Strukturierung und sprachliche Verbesserung von Schreiben, Textbausteinen und internen Arbeitshilfen.
- Zusammenfassung nicht sensibler Sachverhalte oder anonymisierter Fallkonstellationen.
- Erstellung allgemeiner, nicht personenbezogener Vorlagen, Checklisten und Schulungsunterlagen.
- Unterstützung bei Recherche und Plausibilisierung, sofern Ergebnisse fachlich geprüft werden.
- Telefonische Bearbeitung von Anliegen der Mitarbeitenden über den KI-Telefonassistenten fonio.ai (siehe 10.5).

10.2 Unzulässige oder nur nach Freigabe zulässige KI-Nutzung

- Keine Eingabe von Gesundheitsdaten, Diagnosen, Ausweisdokumenten, Arbeitserlaubnissen, Lohnabrechnungen, Bankdaten, Steuer- oder Sozialversicherungsdaten ohne ausdrückliche interne Freigabe.
- Keine automatische Bewertung, Ablehnung oder Priorisierung von Bewerbern oder Mitarbeitenden durch KI, wenn daraus faktisch eine Personalentscheidung folgt.
- Keine KI-generierten Abmahnungen, Kündigungen oder arbeitsrechtlich erheblichen Schreiben ohne menschliche Endprüfung.
- Keine Nutzung privater KI-Konten für personenbezogene Daten aus dem Unternehmen.
- Keine Verwendung von KI-Ausgaben als alleinige Tatsachengrundlage, insbesondere nicht bei Fehlzeiten, Leistung, Verhalten, Vergütung, Disziplinarmaßnahmen oder Einsatzentscheidungen.

10.3 KI im Recruiting und in der Mitarbeitersteuerung

KI-Systeme, die Bewerbungen analysieren, Kandidaten bewerten, Bewerber filtern, Arbeitsbedingungen beeinflussen, Aufgaben zuteilen, Leistung oder Verhalten überwachen oder Kündigungs-/Förderentscheidungen unterstützen, können nach der EU-KI-Verordnung (Verordnung (EU) 2024/1689, Anhang III) in den Hochrisiko-Bereich fallen.

Die jobnext24 GmbH setzt derzeit keine Hochrisiko-KI-Systeme im Sinne der KI-Verordnung ein. Das systemgestützte Matching in zvoove (vgl. 7.1) und der KI-Telefonassistent fonio.ai (vgl. 10.5) dienen ausschließlich der Vorbereitung menschlicher Entscheidungen bzw. der

Kommunikationsunterstützung und stellen keine Hochrisiko-Anwendung dar. Vor einer etwaigen künftigen Nutzung erfolgen eine gesonderte Freigabe, Risikobewertung sowie ggf. eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und eine Bewertung nach der KI-Verordnung.

Matching-, Such-, Filter-, Automatisierungs- und KI-Funktionen dürfen nur vorbereitend genutzt werden. Die verantwortliche Entscheidung trifft immer ein Mensch. Betroffene können eine menschliche Überprüfung verlangen, soweit eine KI-gestützte Empfehlung für sie relevant war.

10.4 Transparenz, Schulung und Kontrolle

- Mitarbeitende, die KI-Systeme einsetzen, werden zu Datenschutz, Datenminimierung, Halluzinationsrisiken, Vertraulichkeit, Urheberrecht und Diskriminierungsrisiken geschult.
- KI-Nutzungen mit personenbezogenen Daten werden dokumentiert, risikobasiert bewertet und nur mit freigegebenen Tools durchgeführt.
- Bei ChatGPT/OpenAI werden ausschließlich Business-/Enterprise-Umgebungen mit Data Processing Agreement genutzt; kein Training mit Eingaben.
- Personenbezogene Daten werden vor Eingabe minimiert, anonymisiert oder pseudonymisiert, soweit der Zweck dies erlaubt.
- KI-Ausgaben werden vor Verwendung fachlich und rechtlich plausibilisiert.

10.5 KI-Telefonassistent (fonio.ai) für Mitarbeitende

Zur besseren telefonischen Erreichbarkeit setzen wir den KI-Telefonassistenten fonio.ai ein. Der Assistent nimmt Anrufe von Mitarbeitenden entgegen, versteht das Anliegen und leitet es an die zuständigen Personen weiter oder vermerkt es zur Bearbeitung.

Einsatzbereich (schrittweise Erweiterung)

Aktuell: Erreichbarkeit für Mitarbeitende außerhalb der Bürozeiten.

Schrittweise Erweiterung auf allgemeine Anliegen der Mitarbeitenden während und außerhalb der Bürozeiten (z. B. Krankmeldungen, Verfügbarkeitsabfragen, Einsatz, Urlaub, Lohnfragen).

Bewerber, Interessenten und Kunden werden derzeit NICHT durch fonio.ai bearbeitet. Anrufe dieser Personengruppen werden an einen menschlichen Mitarbeitenden weitergeleitet oder als Nachricht aufgenommen.

Anbieter und Verarbeitung: Der KI-Telefonassistent wird bereitgestellt durch die fonio GmbH (Deutschland). Ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO ist abgeschlossen. Die Verarbeitung erfolgt innerhalb der EU. Personenbezogene Daten werden weder durch fonio noch durch dessen Subprozessoren zum Training, zur Verbesserung oder zur Evaluierung von KI-Modellen verwendet (vertraglich ausgeschlossen).

Datenkategorien:

- Telefonnummer, Uhrzeit, Dauer des Anrufs (Metadaten).
- Sprachliche Äußerungen während des Gesprächs – diese werden LIVE in Text transkribiert; eine dauerhafte Audio-Speicherung der Stimme findet NICHT statt.
- Inhalte der Anliegen (z. B. Krankmeldung, Verfügbarkeit, Rückrufwunsch).
- Ggf. Verknüpfung zu Ihrem Personalstamm, um Sie zu identifizieren und Ihr Anliegen richtig zuzuordnen.

Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG (Durchführung des Beschäftigungsverhältnisses).
- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an effizienter Erreichbarkeit und Kommunikation).
- Bei Gesundheitsdaten (z. B. Krankmeldung): Art. 9 Abs. 2 lit. b DSGVO i. V. m. § 26 Abs. 3 BDSG.

Transparenz und Ihre Rechte beim Anruf:

- Sie erhalten zu Beginn jedes Anrufs den Hinweis, dass Sie mit einem KI-Assistenten sprechen (Art. 50 KI-Verordnung, verbindlich ab 02.08.2026).
- Sie haben jederzeit das Recht, einen menschlichen Ansprechpartner zu verlangen. Der Assistent leitet Sie in diesem Fall weiter oder nimmt Ihren Rückrufwunsch auf.
- Sie können der Nutzung des KI-Assistenten für Ihre Anrufe generell widersprechen; in diesem Fall werden Ihre Anrufe ausschließlich menschlich bearbeitet.
- Es findet keine ausschließlich automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO statt.
- Die Nutzung des Assistenten ist für Sie freiwillig – Sie können jederzeit ausschließlich die regulären Kontaktkanäle (E-Mail, Post, persönliches Gespräch) nutzen.

Speicherung und Löschung:

- Transkribierte Anliegen werden nur so lange gespeichert, wie dies für die Bearbeitung des konkreten Vorgangs erforderlich ist (z. B. Krankmeldung wird in die Personalakte überführt, Rückrufwunsch nach erfolgtem Rückruf gelöscht).
- Metadaten (Anrufzeit, Nummer) werden zur Nachvollziehbarkeit für einen begrenzten Zeitraum aufbewahrt.
- Keine dauerhafte Audio-Speicherung.

10.6 KI-gestützte Kommunikation über WhatsApp/SuperChat

Bei der Kommunikation über WhatsApp Business (SuperChat) nutzen wir KI-gestützte Antwortvorschläge, um Mitarbeitende bei der Beantwortung wiederkehrender Anliegen zu unterstützen.

- Diese Vorschläge werden ausschließlich als Entwurf angezeigt; eine Nachricht wird erst nach Prüfung und Freigabe durch eine Mitarbeiterin oder einen Mitarbeiter

versendet. Es erfolgt keine automatisierte, KI-gesteuerte Versendung ohne menschliche Kontrolle.

- Da die Kommunikation stets durch einen Menschen final geprüft und freigegeben wird, handelt es sich um eine unterstützende KI-Nutzung im Sinne von Ziffer 10.1, nicht um ein eigenständig mit Ihnen interagierendes KI-System.
- Unabhängig davon weisen wir im WhatsApp-Chat transparent darauf hin, dass bei der Beantwortung KI-Unterstützung zum Einsatz kommen kann (Transparenz entsprechend Art. 50 KI-Verordnung, verbindlich ab 02.08.2026).
- Es findet keine ausschließlich automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO statt.

11. Automatisierte Entscheidungsfindung und Profiling

Es findet keine ausschließlich automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO statt, die gegenüber einer betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Insbesondere werden Bewerber nicht ausschließlich automatisiert abgelehnt, Mitarbeitende nicht ausschließlich automatisiert einem Einsatz zugeordnet und arbeitsrechtliche Entscheidungen nicht ausschließlich automatisiert getroffen. Auch der KI-Telefonassistent fonio.ai trifft keine für Sie rechtlich erheblichen Entscheidungen; er nimmt lediglich Anliegen entgegen und leitet sie weiter.

Systemgestützte Such-, Filter-, Matching-, Plausibilitäts-, Automatisierungs- oder Auswertungsfunktionen dienen ausschließlich der Vorbereitung menschlicher Entscheidungen. Werbe-Targeting durch Google Ads und Meta-Pixel erfolgt nur nach Einwilligung und führt nicht zu rechtlich erheblichen Entscheidungen gegenüber betroffenen Personen.

12. Empfänger und Kategorien von Empfängern

Innerhalb der jobnext24 GmbH erhalten nur diejenigen Stellen Zugriff auf personenbezogene Daten, die diese für ihre Aufgaben benötigen. Externe Empfänger erhalten Daten nur, wenn dies rechtlich erlaubt, vertraglich erforderlich, gesetzlich vorgeschrieben oder durch Einwilligung gedeckt ist.

Empfängerkategorie	Typische Daten / Zweck
Kundenunternehmen / Entleiher	Kandidatenprofile, Einsatzdaten, Qualifikationen, Kontaktdaten, Verfügbarkeit, Arbeitszeit-/Leistungsnachweise (nur für Einsatz, Arbeitsschutz, Abrechnung).
Sozialversicherungsträger, Krankenkassen, Finanzamt, Berufsgenossenschaft, Bundesagentur für Arbeit, Behörden	Meldungen, Bescheinigungen, steuer-/sozialversicherungsrechtliche Daten, AÜG-relevante Nachweise.
Banken und Zahlungsdienstleister	Zahlungsdaten für Lohn, Abschläge, Erstattungen, Rechnungen.

Empfängerkategorie	Typische Daten / Zweck
Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, Gerichte, Inkasso	Daten zur Beratung, Prüfung, Rechtsdurchsetzung und Forderungsbearbeitung.
IT- und Softwaredienstleister (Auftragsverarbeiter)	zvoove, SuperChat, WhatsApp/Meta, Brevo (Brevo GmbH/Sendinblue SAS), IONOS, OpenAI (ChatGPT Enterprise), fonio.ai (fonio GmbH), Google (Analytics, Ads, Tag Manager), Adobe, Make (EU), OpenStreetMap, Cookie-Consent-Tool, Hosting-, Support- und Backup-Dienstleister.
Stellenbörsen und Recruiting-Partner	Veröffentlichung von Stellenangeboten und Empfang von Bewerbungen über Portale wie z. B. Bundesagentur für Arbeit, Indeed, Stepstone, LinkedIn, XING.
Lieferanten und Kundenportale	Nur erforderliche Daten für Zugang, Arbeitsschutz oder Vertragsabwicklung.

Auftragsverarbeiter werden nach Art. 28 DSGVO vertraglich verpflichtet und verarbeiten Daten nur nach Weisung der jobnext24 GmbH.

13. Drittlandübermittlungen

Eine Verarbeitung personenbezogener Daten außerhalb der EU oder des EWR erfolgt nur, wenn hierfür eine rechtliche Grundlage und geeignete Garantien bestehen. Dazu gehören insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission, EU-Standardvertragsklauseln, zusätzliche Schutzmaßnahmen oder eine gesetzliche Ausnahme nach Art. 49 DSGVO.

Konkret betreffen Drittlandübermittlungen folgende Anbieter:

- OpenAI LLC, San Francisco, USA – Angemessenheitsbeschluss DPF, SCC; nur Enterprise-Umgebung, kein Training mit Eingaben.
- Google Ireland Limited, Dublin (Übertragung an Google LLC, USA) – SCC + DPF (Participant 5780).
- Meta Platforms Ireland Limited, Dublin (Übertragung an Meta Platforms, Inc., USA) – SCC + DPF (Participant 4452); gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.
- WhatsApp Ireland Limited, Dublin (Übertragung an Meta Platforms, Inc., USA) – SCC + DPF (Participant 7735).
- Adobe Systems Incorporated, San Jose, USA – SCC + DPF (Participant 5660).
- Brevo GmbH (DE) / Sendinblue SAS (FR, EU) – primär EU; bei Subauftragnehmern in Drittländern SCC.
- OpenStreetMap Foundation, Cambridge, Vereinigtes Königreich – Angemessenheitsbeschluss UK.
- Make s.r.o., Prag, Tschechien – EU; kein Drittlandtransfer.

- fonio GmbH, Deutschland – EU; kein Drittlandtransfer.

14. Speicherdauer und Löschung

Wir speichern personenbezogene Daten nur so lange, wie dies für die jeweiligen Zwecke erforderlich ist. Danach werden Daten gelöscht, anonymisiert oder gesperrt, sofern gesetzliche Aufbewahrungs-, Nachweis- oder Verteidigungspflichten nicht entgegenstehen. Die folgenden Fristen sind Regelwerte.

Datenbereich	Regelspeicherdauer
Bewerbungsdaten bei Absage	In der Regel 6 Monate nach Abschluss des Bewerbungsverfahrens (§ 15 Abs. 4 AGG). Bei drohenden Klageverfahren bis zu 3 Jahre (§ 195 BGB).
Bewerberpool / Talentpool	Nur mit Einwilligung; Daten werden spätestens 2 Jahre nach Erteilung der Einwilligung gelöscht.
Personalakte / Beschäftigendaten	Differenzierte Speicherung: Lohnabrechnungs-, Steuer- und Buchungsdokumente unterliegen Aufbewahrungspflichten von 10 Jahren (§ 257 HGB, § 147 AO). Andere Bestandteile (Bewerbungsunterlagen, Leistungsbeurteilungen, Abmahnungen) werden gelöscht, sobald der Verarbeitungszweck entfallen ist; Abmahnungen i. d. R. nach 2-3 Jahren.
Lohnabrechnungs-, Steuer- und Buchungsdaten	10 Jahre (§ 147 AO, § 257 HGB).
Arbeitszeit-, Einsatz- und AÜG-Nachweise	Überlassungsnachweise mind. 2 Jahre (AÜG); abrechnungsrelevante Daten bis zu 10 Jahre.
Gesundheits-/Fehlzeitendaten	Nur solange für Entgeltfortzahlung, Abrechnung, Arbeitsschutz oder Rechtsverteidigung erforderlich; in der Regel nicht länger als 3 Jahre nach Beendigung des Arbeitsverhältnisses.
Kunden-/Interessentendaten	Dauer der Geschäftsbeziehung zzgl. 10 Jahre für buchhalterische Unterlagen; reine Kontaktdaten ohne Vertragsbezug: bis zu 3 Jahre nach letztem Kontakt.
Newsletter-Abonnenten	Bis zum Widerruf; Einwilligungsnachweis (Double-Opt-in-Log) 3 Jahre nach Abmeldung (§§ 195, 199 BGB).
Messenger-/WhatsApp-Kommunikation	Solange für Bearbeitung oder Kundenbetreuung erforderlich; i. d. R. nicht länger als 2 Jahre nach letztem Kontakt.
fonio.ai Anrufmetadaten und Transkripte	Transkribierte Anliegen: nur bis zur Bearbeitung des Vorgangs, dann Überführung in die Personalakte oder Löschung. Anrufmetadaten (Nummer, Zeitpunkt): begrenzter Zeitraum zur Nachvollziehbarkeit. Keine dauerhafte Audio-Speicherung.
Make-Automatisierungen / Protokolle	Solange für Fehleranalyse und Sicherheitsnachweis erforderlich.

Datenbereich	Regelspeicherdauer
Website-Tracking (Google Analytics, Ads, Meta-Pixel)	GA4: bis zu 2 Jahre. Google Ads-Cookies: 90 Tage. Meta-Pixel: i. d. R. bis 180 Tage.
Website-Logdaten (IONOS)	In der Regel 7-14 Tage; bei Sicherheitsvorfällen bis zu 90 Tage.
KI-Eingaben und KI-Ergebnisse	Nur solange für Dokumentation oder Qualitätssicherung erforderlich; Eingaben werden minimiert.

15. Pflicht zur Bereitstellung personenbezogener Daten

Die Bereitstellung personenbezogener Daten ist teilweise gesetzlich oder vertraglich erforderlich. Ohne erforderliche Daten können wir Bewerbungen nicht ordnungsgemäß bearbeiten, Arbeitsverhältnisse nicht begründen oder durchführen, Mitarbeitende nicht rechtssicher einsetzen, Lohn nicht abrechnen, gesetzliche Meldungen nicht vornehmen oder Kundenaufträge nicht erfüllen.

Freiwillige Angaben (z. B. Bewerberpool, Fotos, Newsletter, optionale Cookies, Nutzung des KI-Telefonassistenten) können verweigert oder später widerrufen werden, ohne Nachteile. Dies gilt nicht für Daten, die für das Arbeitsverhältnis oder gesetzliche Pflichten erforderlich sind.

16. Einwilligungen und Widerruf

Dieses Dokument selbst ersetzt keine gesonderte Einwilligung. Soweit eine freiwillige Einwilligung erforderlich ist, wird diese separat, transparent und widerruflich eingeholt. Eine pauschale Einwilligung in alle Datenverarbeitungen oder in den Einsatz von KI wird nicht vorausgesetzt.

Soweit wir Verarbeitungen auf eine Einwilligung stützen, ist die Einwilligung freiwillig, informiert und jederzeit mit Wirkung für die Zukunft widerrufbar. Der Widerruf berührt nicht die Rechtmäßigkeit der Verarbeitung bis zum Widerruf.

Im Beschäftigungsverhältnis stützen wir notwendige Verarbeitungen grundsätzlich nicht auf Einwilligung, sondern auf Vertrag (Art. 6 Abs. 1 lit. b DSGVO), § 26 BDSG, gesetzliche Pflichten oder berechnete Interessen.

17. Widerspruchsrecht nach Art. 21 DSGVO

PFLICHTHINWEIS: Ihr Widerspruchsrecht nach Art. 21 DSGVO

Sie haben das Recht, jederzeit aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung Ihrer personenbezogenen Daten, die auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) erfolgt, Widerspruch einzulegen. Dies gilt auch für ein etwaiges Profiling auf Grundlage dieser Bestimmung.

Widerspruch gegen Direktwerbung: Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Ihrer Daten zum Zwecke der Direktwerbung einzulegen. Dieser Widerspruch erfordert keine Begründung.

Widerspruch richten Sie an: a.fiege@jobnext24.de (Betreff: Widerspruch Datenschutz).

18. Rechte der betroffenen Personen

- Auskunft über die verarbeiteten personenbezogenen Daten (Art. 15 DSGVO).
- Berichtigung unrichtiger oder unvollständiger Daten (Art. 16 DSGVO).
- Löschung personenbezogener Daten (Art. 17 DSGVO), soweit keine Aufbewahrungs- oder Nachweispflichten entgegenstehen.
- Einschränkung der Verarbeitung (Art. 18 DSGVO).
- Datenübertragbarkeit (Art. 20 DSGVO), soweit anwendbar.
- Widerspruch gegen Verarbeitungen auf Grundlage berechtigter Interessen (Art. 21 DSGVO) – siehe Abschnitt 17.
- Widerruf erteilter Einwilligungen mit Wirkung für die Zukunft (Art. 7 Abs. 3 DSGVO).
- Nicht einer ausschließlich automatisierten Entscheidung im Sinne von Art. 22 DSGVO unterworfen zu werden.
- Erläuterung des Matching-Ergebnisses bei Nutzung systemgestützter Such- und Filterfunktionen.
- Anspruch auf menschlichen Ansprechpartner beim KI-Telefonassistenten fonio.ai (vgl. 10.5).

Geltendmachung der Rechte: Nachricht an a.fiege@jobnext24.de mit Betreff Datenschutz.

Die Bearbeitung erfolgt grundsätzlich kostenfrei und innerhalb eines Monats (Art. 12 Abs. 3 DSGVO); diese Frist kann bei komplexen Anträgen um zwei weitere Monate verlängert werden. Bei begründeten Zweifeln an der Identität können wir einen angemessenen Identitätsnachweis verlangen (Art. 12 Abs. 6 DSGVO).

19. Beschwerderecht bei einer Aufsichtsbehörde

Betroffene Personen haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren. Für die jobnext24 GmbH ist regelmäßig zuständig:

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen)

Prinzenstraße 5, 30159 Hannover – Telefon: 0511 120-4500 – E-Mail:
poststelle@lfid.niedersachsen.de – Website: www.lfd.niedersachsen.de

20. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Wir treffen angemessene technische und organisatorische Maßnahmen, um personenbezogene Daten zu schützen:

- Rollen- und Berechtigungskonzepte in zvoove, Payroll, SuperChat, Make, fonio.ai, E-Mail und Dateiablage.
- Zugriffsbeschränkung nach dem Need-to-know-Prinzip.
- Passwort- und Authentifizierungsregeln; soweit verfügbar Mehr-Faktor-Authentifizierung.
- SSL/TLS-Verschlüsselung der Website und Datenübertragung.
- Verschlüsselung bei Übertragung und Speicherung, soweit technisch verfügbar.
- Protokollierung und Nachvollziehbarkeit relevanter Systemzugriffe.
- Backups, Wiederherstellungsverfahren und Schutz vor Schadsoftware.
- Vertraulichkeitsverpflichtungen und regelmäßige Datenschutz-/KI-Schulungen.
- Vertragliche Verpflichtung von Auftragsverarbeitern und Prüfung von Unterauftragsverarbeitern.
- Lösch- und Sperrkonzept für Bewerberdaten, Personalakten und nicht mehr benötigte Kommunikationsdaten.
- Melde- und Reaktionsprozess für Datenschutzverletzungen nach Art. 33, 34 DSGVO.
- Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO bei umfangreicher Verarbeitung besonderer Datenkategorien.

21. Datenschutz im Arbeitsalltag – Hinweise für Mitarbeitende

Hinweis zur Verbindlichkeit

Die nachfolgenden Hinweise beschreiben den datenschutzkonformen Umgang mit personenbezogenen Daten bei der Nutzung unserer Systeme. Ihre rechtliche Verbindlichkeit für interne Mitarbeitende ergibt sich aus der separaten internen Weisung Datenschutz, die vor Ort ausgehändigt und auf diese Datenschutzhinweise verweist.

- Personenbezogene Daten werden grundsätzlich in den freigegebenen Fachsystemen dokumentiert, nicht in privaten Dateien oder Accounts.
- Freitextnotizen müssen sachlich, erforderlich, wahrheitsgemäß und gerichtsfest formuliert sein; unsachliche, wertende oder diskriminierende Formulierungen sind unzulässig.
- Messenger-Kommunikation (SuperChat, WhatsApp) und KI-Telefonassistent (fonio.ai) dienen der schnellen Kommunikation, nicht der dauerhaften Personalakte für sensible Vorgänge.
- Relevante Entscheidungen und Nachweise werden in zvoove bzw. der vorgesehenen Personal-/Kundenakte dokumentiert.
- KI darf personenbezogene Daten nur erhalten, wenn das Tool freigegeben ist, die Daten minimiert sind und der Zweck dokumentiert ist.

- Make-Automatisierungen dürfen nur freigegebene Systeme verbinden und nur nach interner Freigabe eingesetzt werden.
- Jede KI-Ausgabe, die extern verwendet wird oder Personal-/Kundenbezug hat, muss vor Versand fachlich geprüft werden.
- Lohnabrechnungen, Diagnosen, Ausweisdokumente werden nicht über Messenger versendet.
- Zugriffe und Berechtigungen werden bei Eintritt, Rollenwechsel und Austritt angepasst.

22. Änderungen dieser Datenschutzhinweise

Wir passen diese Datenschutzhinweise an, wenn sich unsere Datenverarbeitung, eingesetzte Systeme, Rechtsgrundlagen, Rechtsprechung oder aufsichtsbehördliche Anforderungen ändern. Die jeweils aktuelle Version wird auf unserer Website bereitgestellt.

Diese Datenschutzhinweise sind eine öffentliche Downloadfassung der jobnext24 GmbH. Interne Nachweise, Vertragsunterlagen, Prüfvermerke und Freigaben werden getrennt geführt und sind nicht Bestandteil dieser öffentlichen Fassung.