Auftragsverarbeitungsvertrag (AVV)

Stand: 14. Juli 2026

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO") zwischen dem Kunden als Verantwortlichem (nachfolgend „Verantwortlicher" oder „Auftraggeber") und Martin Watzlaw, NEXUS Communication (Geschäftsbezeichnung), IT Softwareentwickler und Berater, Gutenbergstr. 24, 61191 Rosbach vor der Höhe (nachfolgend „Auftragsverarbeiter" oder „Anbieter"), als Auftragsverarbeiter. Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE204671098. Weitere Angaben im Impressum. Dieser Auftragsverarbeitungsvertrag (AVV) ist Bestandteil des zwischen den Parteien geschlossenen Nutzungsvertrags über die Software besetzo (siehe AGB) und konkretisiert die datenschutzrechtlichen Pflichten der Parteien für die im Rahmen dieses Vertrags erfolgende Verarbeitung personenbezogener Daten.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Anbieter stellt dem Auftraggeber die internetbasierte Software besetzo zur Personal-, Schicht- und Einsatzplanung sowie zur Disposition als Software-as-a-Service (SaaS) bereit. Im Rahmen dieser Leistung verarbeitet der Anbieter personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers (Art. 28 DSGVO).
(2) Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Für die von ihm in die Software eingegebenen Daten der eingeplanten Beschäftigten, Disponenten und Subunternehmer ist allein der Auftraggeber verantwortlich. Dies umfasst insbesondere die Prüfung einer Rechtsgrundlage für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und die Beschränkung der Eingaben auf das erforderliche Maß.
(3) Die Dauer dieses Auftrags entspricht der Laufzeit des zugrunde liegenden Nutzungsvertrags. Eine Kündigung des Nutzungsvertrags gilt zugleich als Kündigung dieses AVV. Eine Kündigung dieses AVV allein ist nicht möglich; die Pflichten zur Löschung bzw. Rückgabe nach Vertragsende (§ 9) bleiben bis zu ihrer Erfüllung bestehen.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen

(1) Gegenstand und Zweck der Verarbeitung sind ausschließlich die Bereitstellung und der Betrieb der Software besetzo zur Personal- und Einsatzplanung sowie die damit verbundenen technischen Leistungen (Speicherung, Hosting, Authentifizierung, Sicherung). Eine weitergehende Nutzung der Kundeninhalte zu eigenen Zwecken des Anbieters findet nicht statt. Vertrags-, Abrechnungs-, Sicherheits- und Service-Metadaten, für die der Anbieter selbst Verantwortlicher ist, fallen nicht unter die Auftragsverarbeitung; für sie gilt die Datenschutzerklärung.
(2) Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (im Rahmen der eingesetzten Sub-Auftragsverarbeiter), Einschränken, Löschen und Vernichten personenbezogener Daten mittels der Software.
(3) Art der Daten (Datenkategorien): insbesondere Stammdaten (Name, Kontaktdaten), Planungs- und Einsatzdaten (Verfügbarkeiten, Schichten, Positionen, Bereiche, Projekte), Qualifikations- und Zuordnungsdaten, Beschäftigungs-, Abrechnungs-, Bank-, Sozialversicherungs- und Identitätsdaten, Fehlzeiten sowie Nutzungs- und Anmeldedaten. Freitextfelder und Fehlzeitangaben können besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, insbesondere Gesundheitsdaten, enthalten. Die konkreten Datenarten ergeben sich aus Anlage 1.
(4) Kategorien betroffener Personen: die vom Auftraggeber eingeplanten Beschäftigten, Disponenten, Selbstbucher sowie Beschäftigte etwaiger Subunternehmer des Auftraggebers.

§ 3 Weisungsrecht des Verantwortlichen

(1) Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet; in einem solchen Fall teilt der Anbieter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).
(2) Die Weisungen werden anfänglich durch diesen Vertrag und die Leistungsbeschreibung festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden (Einzelweisungen). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
(3) Der Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Anbieter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

§ 4 Vertraulichkeit

(1) Der Anbieter setzt zur Auftragsverarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
(2) Der Anbieter stellt sicher, dass die zur Verarbeitung befugten Personen die personenbezogenen Daten nur entsprechend der Weisung des Auftraggebers einschließlich der in diesem Vertrag geregelten Befugnisse verarbeiten, sofern sie nicht nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

§ 5 Technische und organisatorische Maßnahmen (TOM)

(1) Der Anbieter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, und hält diese während der Vertragsdauer ein. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage 2 beschrieben.
(2) Der Anbieter ist berechtigt, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Inanspruchnahme weiterer Auftragsverarbeiter (Sub-Auftragsverarbeiter)

(1) Der Auftraggeber erteilt dem Anbieter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Sub-Auftragsverarbeiter) zur Erbringung der Leistung einzusetzen (Art. 28 Abs. 2 Satz 1 DSGVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Sub-Auftragsverarbeiter sind in Anlage 3 aufgeführt; der Auftraggeber genehmigt deren Einsatz mit Abschluss dieses Vertrags.
(2) Beabsichtigt der Anbieter, einen weiteren Sub-Auftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, informiert er den Auftraggeber hierüber vorab in Textform mit einer Frist von mindestens fünf Kalendertagen vor dem geplanten Einsatz. Erhält der Anbieter selbst eine kürzere Vorabinformation oder ist eine kurzfristige Änderung zur Abwehr einer konkreten Sicherheitsgefahr erforderlich, informiert er den Auftraggeber unverzüglich nach Kenntnis. Der Auftraggeber kann dem beabsichtigten Wechsel aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Im Fall eines berechtigten Widerspruchs steht dem Anbieter ein Sonderkündigungsrecht zu, sofern eine einvernehmliche Lösung nicht gefunden wird.
(3) Der Anbieter verpflichtet jeden Sub-Auftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen, insbesondere auf die nach Art. 28 Abs. 4 DSGVO erforderlichen Garantien. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Anbieter gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Sub-Auftragsverarbeiters.
(4) Nicht als Sub-Auftragsverarbeitung im Sinne dieses Paragraphen gelten Nebenleistungen, die der Anbieter als reine Hilfsleistung in Anspruch nimmt (z. B. Telekommunikations-, Wartungs- oder Reinigungsleistungen). Der Anbieter ist gleichwohl verpflichtet, auch hierbei angemessene Vorkehrungen zum Schutz der Daten zu treffen.

§ 7 Drittlandübermittlung

(1) Die primäre Datenbank-, Authentifizierungs- und Speicherverarbeitung erfolgt bei Supabase in Frankfurt am Main (eu-central-1). Vercel-Serverfunktionen werden primär in Frankfurt (fra1) ausgeführt. Das globale Content-Delivery-Netz, technische Protokolle, Sicherungskopien, Supportzugriffe und die Anbieterorganisationen können jedoch zu einer Verarbeitung außerhalb der EU bzw. des EWR führen.
(2) Eine Übermittlung personenbezogener Daten in ein Drittland (Staat außerhalb der EU bzw. des EWR) findet nur statt, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO, z. B. EU-US Data Privacy Framework) oder geeigneter Garantien (Art. 46 DSGVO, insbesondere EU-Standardvertragsklauseln). Etwaige Drittlandbezüge der eingesetzten Sub-Auftragsverarbeiter sind in Anlage 3 ausgewiesen.

§ 8 Unterstützungspflichten des Anbieters

(1) Der Anbieter unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO). Wendet sich eine betroffene Person unmittelbar an den Anbieter, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter.
(2) Der Anbieter unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Benachrichtigung betroffener Personen sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 28 Abs. 3 lit. f DSGVO), jeweils unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.
(3) Wird dem Anbieter eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt, informiert er den Auftraggeber unverzüglich, damit dieser seinen Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO nachkommen kann.

§ 9 Löschung und Rückgabe nach Beendigung der Verarbeitung

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Anbieter nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 3 lit. g DSGVO).
(2) Der Anbieter stellt dem Auftraggeber nach Vertragsende die vom Auftraggeber eingegebenen Daten für einen Zeitraum von 30 Kalendertagen in einem gängigen, maschinenlesbaren Format zum Export bereit. Danach werden die Daten gemäß Absatz 1 gelöscht. Der Anbieter bestätigt dem Auftraggeber die auftragsgemäße Löschung auf Anfrage in Textform.
(3) Die gesetzlichen Aufbewahrungsfristen, die den Auftraggeber als Verantwortlichen treffen (insbesondere arbeitszeit-, lohn-, steuer- und sozialversicherungsrechtliche Aufbewahrungspflichten), bleiben unberührt. Der Auftraggeber ist dafür verantwortlich, vor der endgültigen Löschung die zur Erfüllung dieser Pflichten erforderlichen Daten zu exportieren bzw. zu sichern.

§ 10 Nachweise und Kontrollen

(1) Der Anbieter stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei (Art. 28 Abs. 3 lit. h DSGVO).
(2) Der Nachweis kann auch durch geeignete Zertifizierungen, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Auditoren) oder durch eine geeignete Zertifizierung nach Art. 42 DSGVO geführt werden.
(3) Vor-Ort-Kontrollen sind mit angemessener Vorankündigung, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs durchzuführen. Sie dürfen die Betriebs- und Geschäftsgeheimnisse sowie den Schutz der Daten anderer Kunden des Anbieters nicht beeinträchtigen.

§ 11 Mitteilungspflichten und Haftung

(1) Der Anbieter teilt dem Auftraggeber unverzüglich Verstöße gegen Datenschutzvorschriften oder gegen die im Auftrag getroffenen Festlegungen mit, soweit sie die Verarbeitung im Auftrag betreffen.
(2) Für die Haftung im Verhältnis der Parteien gelten die Regelungen des zugrunde liegenden Nutzungsvertrags (AGB) ergänzend; im Außenverhältnis gegenüber betroffenen Personen gilt Art. 82 DSGVO.

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen der Parteien, insbesondere den AGB, gehen die Regelungen dieses AVV hinsichtlich der Verarbeitung personenbezogener Daten vor.
(2) Änderungen und Ergänzungen dieses Vertrags und seiner Anlagen bedürfen mindestens der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.
(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
(4) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 - Datenarten und Kategorien betroffener Personen

Datenarten: Personenstamm- und Kontaktdaten einschließlich Name, Geschlecht, Geburtsdatum, Geburtsort, Geburtsname, Staatsangehörigkeit, Anschrift, Telefon und E-Mail-Adresse; Beschäftigungs-, Personalnummern-, Qualifikations-, Führerschein-, Ausweis- und Dienstausweisdaten; Abrechnungs- und Bankdaten einschließlich Verdienstgrenzen, Sozialversicherungsnummer, Krankenkasse, IBAN, BIC und Bank; Anmelde- und Zugangsdaten einschließlich E-Mail-Adresse, Rolle, Anmeldezeitpunkte, IP-Adresse und Sicherheitsereignisse; Planungs- und Einsatzdaten einschließlich Verfügbarkeiten, Fehlzeiten, Schichten, Positionen, Bereiche, Projekte, Zuordnungen, Buchungsstatus und Bemerkungen; Partner- und Subunternehmer-Zuordnungen sowie technische Protokoll- und Metadaten.
Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO können insbesondere durch Fehlzeitarten, Fehlzeitbemerkungen, Krankenkassenangaben oder freie Eingaben entstehen. Der Schutzbedarf wird deshalb als hoch behandelt.
Kategorien betroffener Personen: Beschäftigte, frühere Beschäftigte, Bewerber, Disponenten, Kontoinhaber, Selbstbucher, Ansprechpartner von Kunden und Partnern sowie Beschäftigte von Subunternehmern des Auftraggebers.

Anlage 2 - Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die folgende Beschreibung gibt den technischen Stand vom 14. Juli 2026 wieder. Maßgeblich sind ergänzend die TOM der eingesetzten Sub-Auftragsverarbeiter.

Vertraulichkeit: Zugangskontrolle über individuelle Benutzerkonten mit Passwortauthentifizierung; für Kontoinhaber ist die Einrichtung eines zweiten Faktors verpflichtend, für Plattform-Administratoren zusätzlich eine auf MFA hochgestufte Sitzung erforderlich, für andere Rollen ist MFA optional; Zugriffskontrolle über zeilenbasierte Berechtigungen (Row Level Security), die den Zugriff strikt auf das eigene Konto (Tenant) beschränken; rollenbasierte Rechte (Inhaber, Disponent, Selbstbucher); Trennungskontrolle durch mandantengetrennte Datenhaltung je Konto.
Integrität: Übertragungskontrolle durch durchgängige TLS-Verschlüsselung (HTTPS); Eingabekontrolle durch protokollierte Änderungen an sicherheitsrelevanten Daten.
Verfügbarkeit und Belastbarkeit: tägliche Datenbanksicherungen beim Datenbankdienstleister Supabase mit einer Aufbewahrung der letzten sieben Tage im eingesetzten Pro-Tarif; primäre Datenbankregion Frankfurt am Main. Über die Supabase Storage API gespeicherte Dateiobjekte sind nicht Bestandteil dieser Datenbanksicherungen und können aus ihnen nicht wiederhergestellt werden.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:
Datenschutz-Management mit dokumentierten Weisungen; Auftragskontrolle gegenüber Sub-Auftragsverarbeitern; Aktualisierung der Maßnahmen an den Stand der Technik.

Anlage 3 - Genehmigte Sub-Auftragsverarbeiter

Die nachfolgenden Unterauftragnehmer sind mit Abschluss dieses Vertrags genehmigt. Bei Änderungen gilt das Verfahren nach § 6.

Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513 - Datenbank, Authentifizierung und Speicherung. Die Kundendaten werden in der gewählten Region Frankfurt am Main (eu-central-1) gespeichert und primär verarbeitet; Support und Betrieb können einen Drittlandbezug haben. Grundlage sind die Supabase-DPA einschließlich EU-Standardvertragsklauseln.
Vercel Inc., 440 N Barranca Avenue, Suite 4133, Covina, CA 91723, USA - Hosting, Serverfunktionen, technische Protokolle und weltweite Auslieferung über ein Content-Delivery-Netz. Serverfunktionen sind primär auf Frankfurt (fra1) konfiguriert; Vercel nennt in seiner DPA jedoch primäre Verarbeitung in den USA sowie global replizierte Sicherungskopien. Grundlage sind die Vercel-DPA einschließlich EU-Standardvertragsklauseln.
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland - Zahlungsabwicklung und Abonnements. Stripe ist nur soweit Unterauftragnehmer, wie es personenbezogene Daten nach Weisung verarbeitet. Für eigene Zwecke, insbesondere

Betrugsprävention, Geldwäscheprüfung, Abrechnung und gesetzliche Pflichten, handelt Stripe nach seiner DPA und Datenschutzerklärung als eigener Verantwortlicher. Verbundene Unternehmen und Dienstleister können Daten in Drittländern verarbeiten; hierfür gelten die dort genannten Transfergarantien.
Scaleway SAS, 8 rue de la Ville l’Évêque, 75008 Paris, Frankreich - transaktionaler E-Mail-Versand über Transactional Email in der Region Paris (fr-par). Scaleway gibt für diesen Dienst vollständige Speicherung und Verarbeitung innerhalb der Europäischen Union an. Grundlage ist die Scaleway-DPA.

Kontakt

Fragen zu diesem Auftragsverarbeitungsvertrag richten Sie bitte an: besetzo@nexus-com.de. Weitere Angaben im Impressum. Für die Verarbeitung der Daten, für die der Anbieter selbst Verantwortlicher ist, gilt die Datenschutzerklärung.