alphaflow Bewerbermanagement (alphaflow-recruitment)
Auftragsverarbeitungsvertrag

Zwischen
Ihnen / Kunde

und
der alphaflow GmbH
(nachfolgend „alphaflow“)

Die Parteien schließen diesen Vertrag zur Auftragsverarbeitung (AVV) zu den AGB über die Inanspruchnahme der Leistungen der **alphaflow Bewerbermanagement App** (technisch: ***alphaflow-recruitment***):

§ 1 Gegenstand der Verarbeitung & Dauer der Auftragsverarbeitung
Gegenstand und Dauer des Auftrags ergibt sich aus den AGB.

§ 2 Zweck der Verarbeitung
Die Tätigkeit von alphaflow dient folgenden vereinbarten Zwecken:

- Unterstützung bei der Durchführung von Verträgen oder Aufträgen
- Vertrieb oder Versand von Waren oder Erbringung von Leistungen
- Betreuung von Kunden und Geschäftspartnern
- Gewährleistung der ordentlichen und gesetzeskonformen Buchhaltung
- Rechnungsstellung für Waren oder Leistungen
- Pflege und Verwaltung von Beschäftigtendaten
- Dokumentation von Arbeitszeiten
- Zahlung von Gehältern und Löhnen
- Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen
- Dokumentation und Festlegung von Compensations und Benefits für Beschäftigte
- Überwachung betrieblicher Einrichtungen
- Gewährleistung des Zutrittsschutzes
- Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung
- Kommunikation mittels elektronischer Medien
- Ermöglichung der Kontaktierung von Beschäftigten
- Dokumentation von Terminen von Beschäftigten
- Zugangsverwaltung hinsichtlich Technik (einschließlich Telekommunikation, Netzwerk)
- Verwaltung von Berechtigungen
- Verwaltung von Lizenzen / Software Asset Management
- Telekommunikationskostenabrechnung
- Pflege und Verbesserung von Kommunikationsprozessen
- Qualitätssicherung

§ 3 Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten sind Gegenstand des Auftrags:
Folgende Datenarten sind Gegenstand dieses Auftrags:

- Stammdaten (Adressen)
- Personal- und Identifikationsnummern
- Kundenverhaltensdaten
- Vertragsdaten
- Nutzerkennungen
- E-Mails
- Passwörter
- Zugangsdaten

§ 4 Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind Gegenstand des Auftrags:

- Beschäftigte
- Auszubildende und Praktikanten
- freie Mitarbeiter
- Gesellschafter, Organe der Gesellschaft
- Kunden
- Interessenten
- Lieferanten und Dienstleister
- Mieter
- Geschäftspartner
- externe Berater

§ 5 Allgemeines

Dieser AVV findet auf alle unter den AGB stattfindenden Verarbeitungsmaßnahmen personenbezogener Daten durch alphaflow Anwendung.
Der Kunde ist im Rahmen dieses AVV für die Einhaltung der gesetzlichen Bestimmungen über die Rechtmäßigkeit der Offenlegung personenbezogener Daten gegenüber alphaflow sowie für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten allein verantwortlich.
alphaflow handelt im Rahmen der Verarbeitung personenbezogener Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a) DSGVO vor. Mündliche Weisungen des Kunden hat er unverzüglich in Textform zu bestätigen.
Auf Weisung des Kunden berichtigt oder löscht alphaflow die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „Sperrung“).
alphaflow informiert den Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diese AVV verstößt. alphaflow darf die Umsetzung der Weisung solange aussetzen, bis diese vom Kunden in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf alphaflow ablehnen.
alphaflow gewährleistet, dass die mit der Verarbeitung personenbezogener Daten beauftragten Personen die Weisungen des Kunden beachten und sich zur Vertraulichkeit verpflichtet haben. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht nach Beendigung der Verarbeitung fort.

§ 6 Technische & organisatorische Maßnahmen

Die Parteien vereinbaren technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (nachfolgend „Anlage TOM“).

Im Falle von Änderungen der Anlage TOM darf das vereinbarte Schutzniveau nicht unterschritten wird.

§ 7 Mitteilungspflichten bei Datenschutzverletzungen

alphaflow unterrichtet den Kunden unverzüglich, wenn Verletzungen des Schutzes der von alphaflow verarbeiteten personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO im Hoheitsbereich von alphaflow bekannt werden bzw. falls ein konkreter Verdacht einer solchen Datenschutzverletzung bei alphaflow besteht.
alphaflow und der Kunde werden unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung treffen.

§ 8 Drittlandübermittlung

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb der EU und des EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen und nach vorheriger Zustimmung des Kunden in Textform zulässig.

§ 9 Unterauftragsverarbeiter

alphaflow darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „Unterauftragnehmer“) erbringen lassen.
Der Kunde kann der Unterbeauftragung bei Vorliegen eines wichtigen Grundes der Unterbeauftragung in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln an der Integrität des Unterauftragsverarbeiters besteht.
alphaflow wird mit dem Unterauftragsverarbeiter die in diesem AVV getroffenen Regelungen vereinbaren.
Leistungen, die alphaflow als reine Nebenleistung zur Unterstützung der geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt sind keine Unterbeauftragung.

§ 10 Betroffenenrechte und Unterstützung des Kunden

Macht eine betroffene Person seine Betroffenenrechte aus der DSGVO bei einer der Parteien geltend, so hat sie die jeweils andere Partei darüber unverzüglich zu informieren. alphaflow unterstützt den Kunden im Rahmen der Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

§ 11 Kontrollrechte des Kunden

Der Kunde überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von alphaflow. Hierfür kann er z. B. Auskünfte von alphaflow einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen von alphaflow nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu alphaflow steht. Der Kunde wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe von alphaflow dabei nicht unverhältnismäßig stören.
alphaflow verpflichtet sich, dem Kunden auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen von alphaflow erforderlich sind.
alphaflow stellt dem Kunden auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

§ 12 Haftung und Schadenersatz

Kunde und alphaflow haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen.

§ 13 Laufzeit

Die Laufzeit des AVV orientiert sich an der Laufzeit der AGB.

§ 14 Schlussbestimmungen

Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform. Dies gilt auch für Änderungen dieser Klausel. Sollte eine Bestimmung dieses AVV ganz oder teilweise unwirksam sein, bleibt dieser AVV im Übrigen unberührt. Anstelle der unwirksamen Bestimmung gilt das Gesetz. Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.

Anlage TOM

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
Die Parteien treffen zum Auftragsverarbeitungsvertrag ergänzend folgende Festlegungen über die alphaflow umzusetzenden technischen und organisatorischen Maßnahmen:

§ 15 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Zutrittskontrolle
Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

- Alarmanlage
- Kameraüberwachung und Aufzeichnung mit Infrarotsystem
- Automatisches Zugangskontrollsystem mit biometrischen Zugangsdaten über Fingerabdruckleser
- Protokollierung sämtlicher Zu- und Ausgänge
- Unterteilung der Flächen in 3 zutrittsgeschützte Räume
- Zugang erfolgt ausschließlich durch Schleusen
- es ist 24x7 Personal vor Ort anwesend
- abgetrennte und gesicherte Räume für Batterien, USV und Stromversorgung
- Automatisches Zugangskontrollsystem mit Chipkarten

Zugangskontrolle
Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

- Zuordnung von Benutzerrechten und Einrichtung eines Benutzerstammsatzes pro Nutzer
- Erstellung von Benutzerprofilen
- differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Passwort vergaben
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Authentifikation mit Benutzernamen und Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie bei Übertragung von Daten
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detektion-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

Trennungskontrolle

Folgende stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische softwareseitige Mandantentrennung
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern und Signaturen
- pseudonymisierte Daten: Trennung der Zuordnungsdatei und der Aufbewahrung in einem getrennten und abgesicherten IT-System
- Interne Mandantenfähigkeit des Systems
- Funktionstrennung von Produktiv- und Testsystem]

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung von Daten erfolgt so, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Es erfolgt eine Pseudonymisierung in folgender Art und Weise: personenbezogene Daten werden von Kundenstammdaten, Umsatzdaten strikt getrennt gehalten. Sofern möglich, werden beim elektronischen Transport die personenbezogenen Daten verschlüsselt.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Einsatz von VPN-Tunneln
- Protokollierungsystem
- Schnittstellenanalyse
- Verschlüsselung der Kommunikationswege
- Verschlüsselung physischer Datenträger bei Transport
- Übertragung mit elektronischer Signatur
- Transportsicherung

Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Kunden stets verfügbar sind:

- redundante unterbrechungsfreie Stromversorgung (USV) mit bis zu 2.1000kVA Leistung, GreenPower USV Systeme von Socomec
- zwei getrennte Stromfeeds durch 2 Unterverteilungen in jedem Rack
- 10kw Stromaufnahme je Rack und mehr möglich
- Notstromversorgung durch 1000kVA Dieselaggregate
- direkter Nachbar des Umspannwerkes
- 3-Stufiger Überspannungsschutz – Grobschutz in Hauptverteilung, Mittel- / Feinschutz in Unterverteilungen, optionaler weiterer Schutz durch kundeneingene Stromanschlußleisten
- VESDA System zur Früherkennung von Rauchentwicklung
- CO2-Feuerlöscher in allen Bereichen sofort griffbereit
- VDS-Alarmanlagen
- direkte Alarmierung des technischen Personals vor Ort sowie externer Mitarbeiter
- Klimatisierung der Serverräume mit einer Mischung aus direkter und indirekter Freikühlung
- Kaltwasserversorgung durch energiesparende Aggregate von Emerson Networks
- Luftaustausch durch Geräte jüngster Generation von Weiss Klimatechnik
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts

- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- belastbares Datensicherungs- und Widerherstellungskonzept vorhanden
- Maßnahen zur Datensicherung (physikalisch / logisch)
- Backup-Verfahren
- Spiegelung von Festplatten mittels Raid-Verfahren
- Einsatz eines Monitoring-Programms
- permanente Überwachung der ordnungsgemäßen Funktionalität
- Einsatz von CWDM Technik für hohe Skalierung der Bandbreiten
- Routing durch moderne Juniper Router
- Coreswitching durch moderne Cisco Switches
- Uplinks wahlweise in 100Mbit, 1GBit oder 10Gbit
- Redundante Netzversorgung durch zahlreiche Carrier wie Tiscali International oder die deutsche Telekom
- Peeringverbindungen an diversen Exchangepunkten wie DECiX, AMSiX, KleyReX, ViX und NIX

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Datenschutzleitbild von alphaflow
- Datenschutz-Richtlinie von alphaflow
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit

Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Kunden verarbeitet werden:

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Verpflichtung der Beschäftigten auf die Vertraulichkeit
- standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern