ein Produkt von

caralegal ISiCO MERANTIX MOMENTUM

cara28

by

caralegal

MERANTIX MOMENTUM

ISiCO

Stand: 29.02.2024

caralegal GmbH

Zusammenfassung

- ☐ In dem Vertrag wird die Genehmigungspflichtigkeit des Einsatzes weiterer Unterauftragsverarbeiter nicht geregelt.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Unterauftragsverarbeiter gemäß den nachfolgenden Absätzen dieser Vereinbarung in Anspruch zu nehmen.*

      Allgemeine Einwilligung: Der Auftragsverarbeiter informiert den Verantwortlichen über den Einsatz von neuen Unterauftragsverarbeitern. Der Verantwortliche kann dem Einsatz innerhalb einer Frist von x Tagen widersprechen.

      Gesonderte Einwilligung: Eine Einschaltung von Unterauftragnehmern bedarf der vorhergehenden schriftlichen, jederzeit widerrufbaren Zustimmung des Verantwortlichen und der Aufnahme in den Appendix B (Liste der Unterauftragnehmer als zusätzliche Auftragsverarbeiter). Der Verantwortliche ist berechtigt, die Zustimmung nach eigenem Ermessen zu verweigern.
- ☐ Es besteht keine Regelung dazu, dass der Auftragsverarbeiter den Unterauftragnehmer dieselben Datenschutzpflichten auferlegen muss, denen er selbst nach diesem Vertrag unterliegt. Eine solche Regelung ist jedoch in Art. 28 Abs. 4 S. 1 DS-GVO verankert und damit dringend in den Vertrag aufzunehmen.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Auftragsverarbeiter erlegt den eingesetzten Unterauftragnehmern dieselben Datenschutzpflichten auf, die in diesem Vertrag geregelt sind.*
- ☐ Die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen bei Anfragen von betroffenen Personen gemäß Art. 12-22 DS-GVO zu unterstützen, ist im Vertrag nicht festgelegt.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO.*

- ☐ Es besteht keine Regelung dazu, dass der Verantwortliche die Einhaltung der Anforderungen des Art. 28 DS-GVO beim Auftragsverarbeiter überprüfen kann.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Auftragnehmer stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann und stellt alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung.*
- ☐ Der Vertrag regelt, dass Weisungen grundsätzlich kostenpflichtig sind. Eine solche Regelung ist unzulässig, da der Auftragnehmer bestimmte Pflichten gegenüber dem Verantwortlichen nicht zur Disposition stellen kann.

  Zulässig wäre lediglich eine Regelung, die besagt, dass Weisungen, die über die vertraglichen Vereinbarungen hinausgehen und nicht erforderlich sind, um Verstöße des Auftragnehmers zu beheben oder zu verhindern, kostenpflichtig sind.

Klauseln, die das Zustandekommen des Vertrags verhindern könnten:

- ☐ In dem Vertrag wird die Genehmigungspflichtigkeit des Einsatzes weiterer Unterauftragsverarbeiter nicht geregelt.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Unterauftragsverarbeiter gemäß den nachfolgenden Absätzen dieser Vereinbarung in Anspruch zu nehmen.*

      Allgemeine Einwilligung: Der Auftragsverarbeiter informiert den Verantwortlichen über den Einsatz von neuen Unterauftragsverarbeitern. Der Verantwortliche kann dem Einsatz innerhalb einer Frist von x Tagen widersprechen.

      Gesonderte Einwilligung: Eine Einschaltung von Unterauftragnehmern bedarf der vorhergehenden schriftlichen, jederzeit widerrufbaren Zustimmung des Verantwortlichen und der Aufnahme in den Appendix B (Liste der Unterauftragnehmer als zusätzliche Auftragsverarbeiter). Der Verantwortliche ist berechtigt, die Zustimmung nach eigenem Ermessen zu verweigern.
  - ○ Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ Es besteht keine Regelung dazu, dass der Auftragsverarbeiter den Unterauftragnehmer dieselben Datenschutzpflichten auferlegen muss, denen er selbst nach diesem Vertrag unterliegt. Eine solche Regelung ist jedoch in Art. 28 Abs. 4 S. 1 DS-GVO verankert und damit dringend in den Vertrag aufzunehmen.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Der Auftragsverarbeiter erlegt den eingesetzten Unterauftragnehmern dieselben Datenschutzpflichten auf, die in diesem Vertrag geregelt sind.*
- ☐ Die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen bei Anfragen von betroffenen Personen gemäß Art. 12-22 DS-GVO zu unterstützen, ist im Vertrag nicht festgelegt.

- Vorgeschlagene Formulierung:
  - *Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO.*
- Markierter Text:

  Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt. 5. VERTRAULICHKEIT 5.1. Zugriffsberechtigung: - Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen. 5.2. Geheimhaltungspflicht: - Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.8.3. Maßnahmen nach einer Datenverletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

☐ Es besteht keine Regelung dazu, dass der Verantwortliche die Einhaltung der Anforderungen des Art. 28 DS-GVO beim Auftragsverarbeiter überprüfen kann.

- Vorgeschlagene Formulierung:
  - *Der Auftragnehmer stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann und stellt alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung.*
- Markierter Text:

  11.1. Kontaktinformationen: - Die Parteien können wie folgt kontaktiert werden: - Für den Auftraggebenden: [E-Mail-Adresse] - Für den Auftragnehmenden: [E-Mail-Adresse] 11.2. Mitteilungspflicht bei Kontaktänderungen: - Beide Parteien sind verpflichtet, sich gegenseitig über Änderungen in den Kontaktinformationen zu informieren. 12. BEGINN UND KÜNDIGUNG 12.1. Inkrafttreten des AVV: - Dieser AVV

tritt am Tag der Unterzeichnung durch beide Parteien in Kraft. 12.2. Recht auf Neuverhandlung: - Beide Parteien haben das Recht, eine Neuverhandlung dieses AVV zu verlangen, wenn Gesetzesänderungen oder die Unzweckmäßigkeit der Bestimmungen eine solche

- ☐ Der Vertrag regelt, dass Weisungen grundsätzlich kostenpflichtig sind. Eine solche Regelung ist unzulässig, da der Auftragnehmer bestimmte Pflichten gegenüber dem Verantwortlichen nicht zur Disposition stellen kann.

  Zulässig wäre lediglich eine Regelung, die besagt, dass Weisungen, die über die vertraglichen Vereinbarungen hinausgehen und nicht erforderlich sind, um Verstöße des Auftragnehmers zu beheben oder zu verhindern, kostenpflichtig sind.

  - ○ Markierter Text:

    3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.4.2. Einhaltung des AVV und des Hauptvertrags: - Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt. 4.3. Mitteilung bei rechtlichen Bedenken: - Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich. 4.4. Unterstützung des Auftraggebenden: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und

Klauseln, die Ihre Aufmerksamkeit erfordern:

- ☐ Im Vertrag ist keine Liste der Unterauftragnehmer angefügt. Die Aufnahme einer Liste der Unterauftragnehmer mit Anschrift, Rechtsform und stichwortartiger Beschreibung ihrer Aufgaben ist nicht zwingend notwendig, um den Vertrag abzuschließen, empfiehlt sich aber zu Zwecken der Klarheit und Übersichtlichkeit. Ist diese Liste lediglich verlinkt, empfiehlt sich der Download und die Ablage dieser Liste, um den eigenen Nachweispflichten nachkommen zu können.

  - ○

Vorgeschlagene Formulierung:

- *Der Verantwortliche stimmt hiermit der Beauftragung der in Anlage X genannten Unterauftragnehmer zu.*

- Markierter Text:

Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

☐ Der Vertrag enthält Maßnahmen zur regelmäßigen Evaluation und Überprüfung der eingesetzten TOM. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.

- Markierter Text:

Überwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauf-

tragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

- ☐ Die Maßnahmen zur Pseudonymisierung sind nicht ausreichend im Vertrag enthalten. Obwohl die Pseudonymisierung als mögliche Maßnahme in Art. 32 DS-GVO aufgeführt ist, muss diese jedoch nicht verpflichtend getroffen werden. Hinsichtlich der konkreten Maßnahmen kann dem Auftragsverarbeiter im Rahmen der Angemessenheit vielmehr eine gewisse Flexibilität eingeräumt werden. Fehlen einige der in Art. 32 DS-GVO aufgeführten Maßnahmen in diesem Vertrag, steht das folglich dem Abschluss des Vertrages nicht im Wege.
  - ○ Markierter Text:

    1. Risikobasierter Ansatz: Der Auftragsnehmer kategorisiert Systeme nach Risikostufen, um das erforderliche Sicherheitsniveau zu verwalten und zu kontrollieren. Geringes Risiko: Basisdaten wie Namen, E-Mail-Adressen und Websites. Erfordert Standard-Sicherheits- und Datenschutz-Compliance. Hohes Risiko: Sensible Daten wie Passwörter, Gesundheitsdaten, Kreditkarteninformationen, Bankdaten und Angaben zur sexuellen Orientierung. Erfordert erhöhte Sicherheitsmaßnahmen, Personaltraining, Datenschutz, Zugangskontrolle undÜberwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:

- ☐

Der Vertrag enthält Maßnahmen zum Schutz der Integrität der Daten. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.

- Markierter Text:

  Überwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

☐ Der Vertrag enthält keine Regelung zum Einsatz von Unterauftragsverarbeitern.

- Vorgeschlagene Formulierung:
  - *Für den Einsatz von Unterauftragsverarbeitern müssen Regelungen zur Zulässigkeit des Einsatzes getroffen werden, darunter fällt die Mitteilungspflicht an den Verantwortlichen und die Auferlegung derselben Datenschutzpflichten des Vertrags an den Unterauftragsverarbeiter.*
- Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.

☐ Der Vertrag enthält keine Regelung zur Verarbeitung von besonderen Kategorien personenbezogener Daten. Bitte stellen Sie sicher, dass die Datenverarbeitung auch tatsächlich keine besonderen Kategorien personenbezogener Daten umfasst.

- Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.

☐ Der Vertrag enthält eine Auflistung der von der Datenverarbeitung betroffenen Personengruppen. Bitte stellen Sie sicher, dass die genannten Daten vollständig sind.

- Markierter Text:

Beginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Verarbeitung im Auftrag: - Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. 1.3. Zweck der Datenverarbeitung: - Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitungpersonenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmende verarbeitet die Daten des Auftraggebenden ausschließlich auf Basis der erteilten Weisungen, sofern nicht

gesetzliche Vorschriften der EU oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.

- ☐ Im Vertragstext gibt es keine Bestimmung zur Nutzung der Daten für eigene Zwecke. Folglich ist die Verwendung der Daten für eigene Zwecke untersagt.
  - ○ Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ Der Ort der Datenverarbeitung ist nicht geregelt. Dies ist insbesondere zu empfehlen, damit die Schutzvorkehrungen für die Datenverarbeitung entsprechend angepasst werden können.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Die Verarbeitung und Nutzung der Daten finden ausschließlich in der europäischen Union statt.*
  - ○ Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ Der Vertrag enthält Kategorien der von der Datenverarbeitung betroffenen Personen. Bitte stellen Sie sicher, dass die genannten Kategorien vollständig sind.
  - ○ Markierter Text:

Beginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen und Job-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeit-

sort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitungpersonenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmende verarbeitet die Daten des Auftraggebenden ausschließlich auf Basis der erteilten Weisungen, sofern nicht gesetzliche Vorschriften der EU oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.

- ☐ Der Vertrag enthält Maßnahmen zur Gewährleistung der Belastbarkeit der Systeme. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.
  - ○ Markierter Text:

    Überwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

- ☐ Der Vertrag enthält Maßnahmen zum Schutz der Vertraulichkeit der Daten. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.
  - ○ Markierter Text:

    1. Risikobasierter Ansatz: Der Auftragsnehmer kategorisiert Systeme nach Risikostufen, um das erforderliche Sicherheitsniveau zu verwalten und zu kontrollieren. Geringes Risiko: Basisdaten wie Namen, E-Mail-Adressen und Websites. Erfordert Standard-Sicherheits- und Datenschutz-Compliance. Hohes Risiko: Sensible Daten wie Passwörter, Gesundheitsdaten, Kreditkarteninformationen, Bankdaten und Angaben zur sexuellen Orientierung. Erfordert erhöhte Sicherheitsmaßnahmen, Personaltraining, Datenschutz, Zugangskontrolle undÜberwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

- ☐ Der Vertrag enthält Maßnahmen zur Verschlüsselung der Daten. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.
  - ○ Markierter Text:

1. Risikobasierter Ansatz: Der Auftragsnehmer kategorisiert Systeme nach Risikostufen, um das erforderliche Sicherheitsniveau zu verwalten und zu kontrollieren. Geringes Risiko: Basisdaten wie Namen, E-Mail-Adressen und Websites. Erfordert Standard-Sicherheits- und Datenschutz-Compliance. Hohes Risiko: Sensible Daten wie Passwörter, Gesundheitsdaten, Kreditkarteninformationen, Bankdaten und Angaben zur sexuellen Orientierung. Erfordert erhöhte Sicherheitsmaßnahmen, Personaltraining, Datenschutz, Zugangskontrolle undÜberwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

- ☐ Der Vertrag enthält Maßnahmen zur Gewährleistung der Verfügbarkeit der Systeme. Bitte prüfen Sie die Angemessenheit der Maßnahmen für die konkrete Datenverarbeitung.
  - ○ Markierter Text:

    Überwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrol-

le. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Datenschutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

- ☐ Die Ausnahme von der gesetzlich vorgeschriebenen Mitteilungspflicht ist nicht im Vertrag festgelegt. Dies ist in Art. 28 Abs. 3 S. 2 lit. a DS-GVO vorgesehen.
  - ○ Vorgeschlagene Formulierung:
    - ○ *Eine Mittteilungspflicht besteht explizit dann nicht, wenn aufgrund bestehenden Rechts eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses verboten ist, vgl. Art. 28 Abs. 3 S.2 lit a DS-GVO.*
  - ○ Markierter Text:

Job-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitungpersonenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmende verarbeitet die Daten des Auftraggebenden ausschließlich auf Basis der erteilten Weisungen, sofern nicht gesetzliche Vorschriften der EU

oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.

Klauseln, bei denen Sie beruhigt sein können

- ☐ Der Gegenstand der Verarbeitung ist ausreichend konkret beschrieben.
  - ○ Markierter Text:

    AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmender: [Name des Auftragnehmenden] INHALTSVERZEICHNIS Gegenstand, Dauer, Art und Zweck der Verarbeitung Art der personenbezogenen Daten Rechte und Pflichten des Auftraggebenden Die Rechte und Pflichten des Auftragnehmenden Vertraulichkeit Sicherheit der Verarbeitung Einsatz von Unterauftragnehmenden Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Löschen und Rückgabe von Daten Inspektion und Prüfung Auftraggebende und AuftragnehmendeBeginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Verarbeitung im Auftrag: - Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. 1.3. Zweck der Datenverarbeitung: - Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der

Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der VerarbeitungNeuverhandlung erfordern. 12.3. Kündigungsbedingungen: - Dieser AVV kann gemäß den Bedingungen des Rahmenvertrags gekündigt werden. 13. GELTENDES RECHT 13.1. Anwendbares Recht: - Sofern im Rahmenvertrag nicht anders vereinbart, unterliegt dieser AVV dem deutschen Recht. 14. SONSTIGES 14.1. Aufbewahrung des AVV: - Dieser AVV und alle Anhänge werden in Textform sowie elektronisch von beiden Parteien aufbewahrt. 14.2. Abhängigkeit von Rahmenvertrag: - Dieser AVV und der Rahmenvertrag sind miteinander verbunden und können nicht separatgekündigt werden. Eine Ersetzung dieses AVV durch einen alternativen gültigen AVV ist ohne Kündigung des Rahmenvertrags möglich. 14.3. Vorrang des AVV: - Dieser AVV hat Vorrang vor ähnlichen Bestimmungen in anderen Vereinbarungen zwischen den Parteien, einschließlich des Rahmenvertrags. 14.4. Dokumentation individueller Weisungen: - Individuelle Weisungen nach Abschluss dieses AVV bedürfen der Textform und sind von beiden Parteien zu dokumentieren. 14.5. Freistellung von weiteren Verpflichtungen: - Dieser AVV befreit den Auftragnehmenden nicht von Verpflichtungen, die ihm gemäß der DSGVO oder anderen Rechtsvorschriften obliegen.14.6. Ausschluss des Zurückbehaltungsrechts: - Ein Zurückbehaltungsrecht im Sinne des § 273 BGB hinsichtlich der für den Auftraggebenden verarbeiteten Daten wird hiermit ausgeschlossen. 14.7. Durchsetzbarkeit einzelner Bestimmungen: - Sollte eine Bestimmung dieses Vertrags nicht durchsetzbar sein, so wird die Durchsetzbarkeit der übrigen Bestimmungen hierdurch nicht berührt. 15. UNTERSCHRIFTEN Im Namen des Auftraggebenden: _____ [Unterschrift] Im Namen des Auftragnehmenden: _____ [Unterschrift] [Datum] ANHANG A: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

☐ Die Dauer der Verarbeitung ist ausreichend konkret geregelt.

- Markierter Text:

  AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmender: [Name des Auftragnehmenden] INHALTSVERZEICHNIS Gegenstand, Dauer, Art und Zweck der Verarbeitung Art der personenbezogenen Daten Rechte und Pflichten des Auftraggebenden Die Rechte und Pflichten des Auftragnehmenden Vertraulichkeit Sicherheit der Verarbeitung Einsatz von Unterauftragnehmenden Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Löschen und Rückgabe von Daten Inspektion und Prüfung Auftraggebende und AuftragnehmendeBeginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser

Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Verarbeitung im Auftrag: - Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. 1.3. Zweck der Datenverarbeitung: - Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der VerarbeitungNeuverhandlung erfordern. 12.3. Kündigungsbedingungen: - Dieser AVV kann gemäß den Bedingungen des Rahmenvertrags gekündigt werden. 13. GELTENDES RECHT 13.1. Anwendbares Recht: - Sofern im Rahmenvertrag nicht anders vereinbart, unterliegt dieser AVV dem deutschen Recht. 14. SONSTIGES 14.1. Aufbewahrung des AVV: - Dieser AVV und alle Anhänge werden in Textform sowie elektronisch von beiden Parteien aufbewahrt. 14.2. Abhängigkeit von Rahmenvertrag: - Dieser AVV und der Rahmenvertrag sind miteinander verbunden und können nicht separatgekündigt werden. Eine Ersetzung dieses AVV durch einen alternativen gültigen AVV ist ohne Kündigung des Rahmenvertrags möglich. 14.3. Vorrang des AVV: - Dieser AVV hat Vorrang vor ähnlichen Bestimmungen in anderen Vereinbarungen zwischen den Parteien, einschließlich des Rahmenvertrags. 14.4. Dokumentation individueller Weisungen: - Individuelle Weisungen nach Abschluss dieses AVV bedürfen der Textform und sind von beiden Parteien zu dokumentieren. 14.5. Freistellung von weiteren Verpflichtungen: - Dieser AVV befreit den Auftragnehmenden nicht von Verpflichtungen, die ihm gemäß der DSGVO oder anderen Rechtsvorschriften obliegen.14.6. Ausschluss des Zurückbehaltungsrechts: - Ein Zurückbehaltungsrecht im Sinne des § 273 BGB hinsichtlich der für den Auftraggebenden verarbeiteten Daten wird hiermit ausgeschlossen. 14.7. Durchsetzbarkeit einzelner Bestimmungen: - Sollte eine Bestimmung dieses Vertrags nicht durchsetzbar sein, so wird die Durchsetzbarkeit der übrigen Bestimmungen hierdurch nicht berührt. 15. UNTERSCHRIFTEN Im Namen des Auftraggebenden: _____ [Unterschrift] Im Namen des Auftrag-

nehmenden: _____ [Unterschrift] [Datum] ANHANG A: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

☐ Der Vertrag enthält eine Regelung, dass die Datenverarbeitung nur aufgrund von Weisungen des Verantwortlichen erfolgen darf.

Diese Klausel ist von großer Bedeutung, da sie die klare Verantwortungsverteilung in Bezug auf die Datenverarbeitung festlegt. Sie stellt sicher, dass der Auftragsverarbeiter die personenbezogenen Daten nur im Rahmen der ausdrücklichen Anweisungen des Verantwortlichen verarbeiten darf.

○ Markierter Text:

Beginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Verarbeitung im Auftrag: - Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. 1.3. Zweck der Datenverarbeitung: - Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitung personenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmende verarbeitet die Daten des

Auftraggebenden ausschließlich auf Basis der erteilten Weisungen, sofern nicht gesetzliche Vorschriften der EU oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.4.2. Einhaltung des AVV und des Hauptvertrags: - Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt. 4.3. Mitteilung bei rechtlichen Bedenken: - Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich. 4.4. Unterstützung des Auftraggebenden: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und

- ☐ Der Vertrag enthält keine Haftungsregelung, somit gilt die allgemeine Haftung nach Art. 82 DS-GVO.
- ☐ Der Vertrag enthält keine weiteren Klauseln, die mit unzumutbaren Risiken für den Verantwortlichen einhergehen.
- ☐ Im Vertrag werden keine Dienstleistungen pauschal vom Begriff der Auftragsverarbeitung ausgenommen.
- ☐ Die Art und der Zweck der Datenverarbeitung sind ausreichend konkret beschrieben.
  - ○ Markierter Text:

    AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmender: [Name des Auftragnehmenden] INHALTSVERZEICHNIS Gegenstand, Dauer, Art und Zweck der Verarbeitung Art der personenbezogenen Daten Rechte und Pflichten des Auftraggebenden Die Rechte und Pflichten des Auftragnehmenden Vertraulichkeit Sicherheit der Verarbeitung Einsatz von Unterauftragnehmenden Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Löschen und Rückgabe von Daten Inspektion und Prüfung Auftraggebende und AuftragnehmendeBeginn und Kündigung Geltendes Recht Sonstiges Unterschriften Anhang A: Technische und organisatorische Maßnahmen 1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG 1.1. Zweck und Rahmen des AVV: - Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrund-

verordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden. 1.2.Verarbeitung im Auftrag: - Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. 1.3. Zweck der Datenverarbeitung: - Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind.Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rahmenvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitung

- ☐ Der Auftragsverarbeiter verpflichtet sich zur Unterstützung bei der Benachrichtigung der betroffenen Person(en) gemäß Art. 34 DS-GVO.
  - ○ Markierter Text:

    Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt. 5. VERTRAULICHKEIT 5.1. Zugriffsberechtigung: - Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen. 5.2. Geheimhaltungspflicht: - Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.DATEN 8.1. Benachrichtigungspflicht: - Bei einer Datenschutzverletzung im Bereich des Auftragnehmenden oder eines Unterauftragnehmenden, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmende den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Meldung solcher Vorfälle an die zuständigen Aufsichtsbehörden, unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.8.3. Maßnahmen nach einer Daten-

verletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

☐ Dem Vertrag hängt eine Auflistung der umgesetzten TOM an.

- Markierter Text:

1. Risikobasierter Ansatz: Der Auftragsnehmer kategorisiert Systeme nach Risikostufen, um das erforderliche Sicherheitsniveau zu verwalten und zu kontrollieren. Geringes Risiko: Basisdaten wie Namen, E-Mail-Adressen und Websites. Erfordert Standard-Sicherheits- und Datenschutz-Compliance. Hohes Risiko: Sensible Daten wie Passwörter, Gesundheitsdaten, Kreditkarteninformationen, Bankdaten und Angaben zur sexuellen Orientierung. Erfordert erhöhte Sicherheitsmaßnahmen, Personaltraining, Datenschutz, Zugangskontrolle undÜberwachung. 2. Maßnahmen von Unterprozessoren: Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden. 3. Maßnahmen von Auftragsnehmer: 3.1 Geheimhaltung und Verschlüsselung: Physischer Zugriff auf Datenverarbeitungsgeräte: - Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle. - Büro des Auftragsnehmers: - Eingangstüren stets verschlossen. - Individuelle Zugangsberechtigung und Alarmanlage. - Verwendung von Datenverarbeitungsgeräten: - Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN). - Netzwerkabschottung durch Firewall. - Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen.3.2 Integrität: Weitergabekontrolle: - Kein Zugang für Besucher zum Firmen-LAN/WLAN. - Einsatz elektronischer Signaturen. - Sichere Speicherung und Verarbeitung in Rechenzentren. - Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN). - Dokumentation von Datenübermittlungen. - Eingabekontrolle: - Protokollierung von Dateneingaben, Änderungen und Löschungen. - Protokollierung von Zugangsversuchen. - Überwachung von Systemadministratoren und Benutzeraktivitäten. - Sicherung der Protokolldaten. 4. Verfügbarkeit und Belastbarkeit: - Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust. - Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates. 5. Verfahren zur regelmäßigen Überprüfung und Bewertung:Auftragskontrolle: - Sorgfältige Auswahl der Auftragnehmer. - Klare vertragliche Regelungen zur Datenverarbeitung. - Formalisiertes Instruktionsmanagement. - Schriftliche Erteilung von Weisungen. - Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten. - Datenschutz-Management: - Bestellung eines qualifizierten Datenschutzbeauftragten. - Dokumentiertes Daten-

schutzmanagementsystem. - Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im Datenschutz.

☐ Eine Verarbeitung außerhalb der EU/EWR durch den Auftragsverarbeiter selbst ist vertraglich nicht vorgesehen.

- ○ Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.

☐ Der Auftragsverarbeiter verpflichtet sich zur Unterstützung bei der Meldung von Datenschutzvorfällen an die zuständige Behörde gemäß Art. 33 DS-GVO.

- ○ Markierter Text:

DATEN 8.1. Benachrichtigungspflicht: - Bei einer Datenschutzverletzung im Bereich des Auftragnehmenden oder eines Unterauftragnehmenden, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmende den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Meldung solcher Vorfälle an die zuständigen Aufsichtsbehörden, unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.8.3. Maßnahmen nach einer Datenverletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

☐ Der Auftragsverarbeiter ist zur Löschung bzw. Rückgabe der Daten nach Abschluss der Erbringung der Verarbeitungsleistungen verpflichtet.

- ○ Markierter Text:

DATEN 8.1. Benachrichtigungspflicht: - Bei einer Datenschutzverletzung im Bereich des Auftragnehmenden oder eines Unterauftragnehmenden, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmende den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Meldung solcher Vorfälle an die zuständigen Aufsichtsbehörden, unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.8.3. Maßnahmen nach einer Datenverletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Dat-

en zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.9.2. Kosten für Rückgabe oder Löschung: - Kosten, die im Zusammenhang mit der Rückgabe oder Löschung personenbezogener Daten entstehen, trägt der Auftraggebende. 10. INSPEKTION UND PRÜFUNG 10.1. Zugang zu Informationen und Auditierung: - Der Auftragnehmende stellt dem Auftraggebenden alle erforderlichen Informationen zur Verfügung, um die Einhaltung der Anforderungen von Artikel 28 DSGVO und dieses AVV zu demonstrieren. 10.2. Zugang für Aufsichtsbehörden: - Der Auftragnehmende gewährt den Aufsichtsbehörden, die gemäß geltendem Recht Zugang zu den Einrichtungen des Auftraggebenden und des Auftragnehmenden haben, oder deren Vertretern den erforderlichen Zugang zu seinen physischen Einrichtungen. 11. AUFTRAGGEBENDE UND AUFTRAGNEHMENDE11.1. Kontaktinformationen: - Die Parteien können wie folgt kontaktiert werden: - Für den Auftraggebenden: [E-Mail-Adresse] - Für den Auftragnehmenden: [E-Mail-Adresse] 11.2. Mitteilungspflicht bei Kontaktänderungen: - Beide Parteien sind verpflichtet, sich gegenseitig über Änderungen in den Kontaktinformationen zu informieren. 12. BEGINN UND KÜNDIGUNG 12.1. Inkrafttreten des AVV: - Dieser AVV tritt am Tag der Unterzeichnung durch beide Parteien in Kraft. 12.2. Recht auf Neuverhandlung: - Beide Parteien haben das Recht, eine Neuverhandlung dieses AVV zu verlangen, wenn Gesetzesänderungen oder die Unzweckmäßigkeit der Bestimmungen eine solche

- ☐ Der Auftragsverarbeiter verpflichtet sich zur Unterstützung bei der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO.
  - ○ Markierter Text:

angemessen ist. Hierzu gehören Transparenz in der Datenverarbeitung, Löschung von Daten auf Anfrage und die Bereitstellung von Informationen an betroffene Personen. 4.5. Zusammenarbeit bei Anfragen betroffener Personen: - Sollte eine betroffene Person sich direkt an den Auftragnehmenden wenden, informiert dieser den Auftraggebenden und leitet die Anfrage weiter. Der Auftragnehmende interagiert nicht direkt mit der betroffenen Person. 4.6. Ausnahmen von der Unterstützung: - Nicht inbegriffen in der Unterstützung sind Prüfungen durch Dritte oder zusätzliche Zertifizierungen, die vom Auftraggebenden angefordert werden.Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt. 5. VERTRAULICHKEIT 5.1. Zugriffsberechtigung: - Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen. 5.2. Geheimhaltungspflicht: - Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß

Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.6.2. Anpassung der Sicherheitsmaßnahmen: - Der Auftragnehmende darf Sicherheitsmaßnahmen ändern oder anpassen, sofern diese Änderungen das Sicherheitsniveau nicht mindern. Alle wesentlichen Änderungen müssen dokumentiert und vom Auftraggebenden genehmigt werden. 7. EINSATZ VON UNTERAUFTRAGNEHMENDEN 7.1. Anforderungen an Unterauftragnehmende: - Der Auftragnehmende muss die Anforderungen gemäß Artikel 28 Absätze 2 und 4 DSGVO erfüllen, um Unterauftragnehmende zu beauftragen. 7.2. Verantwortlichkeit gegenüber dem Auftraggebenden: - Der Auftragnehmende bleibt gegenüber dem Auftraggebenden für die Einhaltung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmenden verantwortlich.8.3. Maßnahmen nach einer Datenverletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

- ☐ Der Auftragsverarbeiter verpflichtet sich dazu, die Sicherheit der Verarbeitung durch den Einsatz angemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DS-GVO zu gewährleisten
  - Markierter Text:

    Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt. 5. VERTRAULICHKEIT 5.1. Zugriffsberechtigung: - Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen. 5.2. Geheimhaltungspflicht: - Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.6.2. Anpassung der Sicherheitsmaßnahmen: - Der Auftragnehmende darf Sicherheitsmaßnahmen ändern oder anpassen, sofern diese Änderungen das Sicherheitsniveau nicht mindern. Alle wesentlichen Änderungen müssen dokumentiert und vom Auftraggebenden genehmigt werden. 7. EINSATZ VON UNTERAUFTRAGNEHMENDEN 7.1. Anforderungen an Unterauftragnehmende: - Der Auftragnehmende muss die Anforderungen gemäß Artikel 28 Absätze 2 und 4 DSGVO erfüllen, um Unterauftragnehmende zu beauftragen. 7.2. Verantwortlichkeit gegenüber dem Auftraggebenden: - Der Auftragnehmende bleibt gegenüber dem Auftraggebenden für die Einhal-

tung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmenden verantwortlich.

☐ Es sind Fristen für die Unterstützungshandlungen enthalten.

○ Markierter Text:

Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt. 5. VERTRAULICHKEIT 5.1. Zugriffsberechtigung: - Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen. 5.2. Geheimhaltungspflicht: - Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.DATEN 8.1. Benachrichtigungspflicht: - Bei einer Datenschutzverletzung im Bereich des Auftragnehmenden oder eines Unterauftragnehmenden, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmende den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Meldung solcher Vorfälle an die zuständigen Aufsichtsbehörden, unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen.8.3. Maßnahmen nach einer Datenverletzung: - Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen. 9. LÖSCHEN UND RÜCKGABE VON DATEN 9.1. Rückgabe oder Löschung nach Beendigung: - Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

☐ Der Vertrag enthält eine Regelung, nach der Weisungen dokumentiert werden müssen.

Dies ist ein äußerst wichtiger Schritt, um die Transparenz und Nachvollziehbarkeit in Bezug auf die Datenverarbeitung zu gewährleisten.

○ Markierter Text:

Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse. 1.4. Dauer der Verarbeitung: - Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV. 2. ART DER PERSONENBEZOGENEN DATEN 2.1. Datenverarbeitung gemäß Rah-

menvertrag: - Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung. 2.2. Arten von personenbezogenen Daten: - Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen undJob-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitung3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.4.2. Einhaltung des AVV und des Hauptvertrags: - Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt. 4.3. Mitteilung bei rechtlichen Bedenken: - Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich. 4.4. Unterstützung des Auftraggebenden: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar undangemessen ist. Hierzu gehören Transparenz in der Datenverarbeitung, Löschung von Daten auf Anfrage und die Bereitstellung von Informationen an betroffene Personen. 4.5. Zusammenarbeit bei Anfragen betroffener Personen: - Sollte eine betroffene Person sich direkt an den Auftragnehmenden wenden, informiert dieser den Auftraggebenden und leitet die Anfrage weiter. Der Auftragnehmende interagiert nicht direkt mit der betroffenen Person. 4.6. Ausnahmen von der Unterstützung: - Nicht inbegriffen in der Unterstützung sind Prüfungen durch Dritte oder zusätzliche Zertifizierungen, die vom Auftraggebenden angefordert werden.

Klauseln, die nicht eindeutig zugewiesen werden konnten:

- ☐ cara28 konnte nicht feststellen, ob der Vertrag eine Vergütungsregelung zur Unterstützung des Auftragsverarbeiters bei den Maßnahmen nach Art. 32 bis 36 DS-GVO enthält.
  - Vorgeschlagene Formulierung:
    - *Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Pflichten aus Art. 32 bis 36 DS-GVO.*
  -

Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.

- ☐ cara28 konnte nicht feststellen, ob der Auftragsverarbeiter sich verpflichtet seine Beschäftigten der Vertraulichkeit unterliegen.
  - Vorgeschlagene Formulierung:
    - *Der Auftragnehmer setzt bei der Durchführung nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des Vertrages fort.*
  - Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ cara28 konnte nicht feststellen, ob der Vertrag zeitlich alle Verarbeitungen von personenbezogenen Daten abdeckt.
  - Vorgeschlagene Formulierung:
    - *Die Verpflichtung auf den Datenschutz und die Pflicht zur Verschwiegenheit über Geschäftsgeheimnisse besteht über die Vertragsdauer hinaus.*
  - Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ cara28 konnte nicht feststellen, ob der Vertrag eine Regelung zur Remote-Arbeit enthält.
  - Markierter Text: Eine entsprechende Klausel ist im Vertrag nicht enthalten, daher wurde keine Textpassage markiert.
- ☐ cara28 konnte nicht feststellen, ob der Vertrag eine Regelung, nach welcher der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung stellt, enthält.
  - Vorgeschlagene Formulierung:
    - *Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung.*

- Markierter Text:

  angemessen ist. Hierzu gehören Transparenz in der Datenverarbeitung, Löschung von Daten auf Anfrage und die Bereitstellung von Informationen an betroffene Personen. 4.5. Zusammenarbeit bei Anfragen betroffener Personen: - Sollte eine betroffene Person sich direkt an den Auftragnehmenden wenden, informiert dieser den Auftraggebenden und leitet die Anfrage weiter. Der Auftragnehmende interagiert nicht direkt mit der betroffenen Person. 4.6. Ausnahmen von der Unterstützung: - Nicht inbegriffen in der Unterstützung sind Prüfungen durch Dritte oder zusätzliche Zertifizierungen, die vom Auftraggebenden angefordert werden.11.1. Kontaktinformationen: - Die Parteien können wie folgt kontaktiert werden: - Für den Auftraggebenden: [E-Mail-Adresse] - Für den Auftragnehmenden: [E-Mail-Adresse] 11.2. Mitteilungspflicht bei Kontaktänderungen: - Beide Parteien sind verpflichtet, sich gegenseitig über Änderungen in den Kontaktinformationen zu informieren. 12. BEGINN UND KÜNDIGUNG 12.1. Inkrafttreten des AVV: - Dieser AVV tritt am Tag der Unterzeichnung durch beide Parteien in Kraft. 12.2. Recht auf Neuverhandlung: - Beide Parteien haben das Recht, eine Neuverhandlung dieses AVV zu verlangen, wenn Gesetzesänderungen oder die Unzweckmäßigkeit der Bestimmungen eine solche

☐ cara28 konnte nicht feststellen, ob der Vertrag eine Regelung, nach welcher bei gesetzlich vorgeschriebener Abweichung von der Weisung noch vor der Verarbeitung eine Meldung an den Verantwortlichen erfolgen muss, enthält.

- Vorgeschlagene Formulierung:
  - *Der Auftragnehmer verarbeitet die Daten entsprechend den Weisungen des Verantwortlichen, es sei denn, dass er gesetzlich oder aufgrund anderweitiger vertraglicher Vereinbarungen zur Verarbeitung verpflichtet ist.*
- Markierter Text:

  Job-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden. 3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN 3.1. Verantwortlichkeit und Weisungsbefugnis: - Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitungpersonenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmende verarbeitet die Daten des Auftraggebenden ausschließlich auf Basis der erteilten Weisungen, sofern nicht gesetzliche Vorschriften der EU oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden

darüber informieren, sofern dies gesetzlich zulässig ist.3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.4.2. Einhaltung des AVV und des Hauptvertrags: - Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt. 4.3. Mitteilung bei rechtlichen Bedenken: - Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich. 4.4. Unterstützung des Auftraggebenden: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und

- ☐ cara28 konnte nicht feststellen, ob der Vertrag eine Verpflichtung des Auftragsverarbeiters zum Hinweis auf vermeintlich rechtswidrigen Weisungen enthält. (Art. 28 Abs. 3 DS-GVO)
  - Vorgeschlagene Formulierung:
    - *Wenn der Auftragsverarbeiter die Weisung für rechtswidrig hält, wird er den Verantwortlichen unverzüglich darüber informieren.*
  - Markierter Text:

    3.3. Entscheidungsbefugnis über Datenverarbeitung: - Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden. 3.4. Kostenübernahme für zusätzliche Weisungen: - Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten. 4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN 4.1. Dokumentierte Weisungen: - Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.4.2. Einhaltung des AVV und des Hauptvertrags: - Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt. 4.3. Mitteilung bei rechtlichen Bedenken: - Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich. 4.4. Unterstützung des Auftraggebenden: - Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und

Quelldokument

Relativ Schlecht - caralegal AVV für DPA Check Tool (1).pdf

AUFTRAGSVERARBEITUNGSVERTRAG

Zwischen:

Auftraggebender: [Name des Auftraggebenden]

Auftragnehmender: [Name des Auftragnehmenden]

INHALTSVERZEICHNIS

1. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG

1.1. Zweck und Rahmen des AVV:

- Dieser Vertrag, im Folgenden als "AVV" bezeichnet, dient der Sicherstellung, dass beide

Parteien die Bestimmungen des Artikels 28, Absatz 3 der EU-Datenschutzgrundverordnung (DSGVO) einhalten. Er regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmenden im Auftrag des Auftraggebenden.

1.2. Verarbeitung im Auftrag:

- Der Auftragnehmende verarbeitet die personenbezogenen Daten gemäß der Definition des

Art. 4 Nr. 4 DSGVO ausschließlich nach Weisung des Auftraggebenden. Der Umfang der Datenverarbeitung wird durch den Rahmenvertrag festgelegt, wobei der Auftraggebende allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist.

1.3. Zweck der Datenverarbeitung:

- Der Auftragnehmende verarbeitet die Daten ausschließlich zur Erfüllung der Vereinbarungen, die im Rahmenvertrag über die Bereitstellung der Automatisierungsplattform und dazugehörigen Dienstleistungen festgelegt sind. Dies beinhaltet unter anderem CRM-Datenbereinigung und -anreicherung sowie Marktanalyse.

1.4. Dauer der Verarbeitung:

- Die Verarbeitung beginnt mit dem Abschluss des AVV und ist zeitlich nicht begrenzt. Sie erfolgt bis zur Beendigung des AVV.

2. ART DER PERSONENBEZOGENEN DATEN

2.1. Datenverarbeitung gemäß Rahmenvertrag:

- Die Verarbeitung der Daten des Auftraggebenden erfolgt entsprechend den im Rahmenvertrag festgelegten Art und Zweck der Datenverarbeitung.

2.2. Arten von personenbezogenen Daten:

- Verarbeitet werden Daten wie Namen, E-Mail-Adressen, Unternehmensnamen und Job-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeit-sort

sowie freiwillig geteilte Benutzerprofile verarbeitet werden.

2.3. Kategorien von betroffenen Personen:

- Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden, andere

Endbenutzer, Kunden, Partner sowie Kontakte des Auftraggebenden.

3. RECHTE UND PFLICHTEN DES AUFTRAGGEBENDEN

3.1. Verantwortlichkeit und Weisungsbefugnis:

- Der Auftraggebende ist verantwortlich für die Einhaltung der DSGVO bei der Verarbeitung

personenbezogener Daten. Er ist zudem berechtigt und verpflichtet, dem Auftragnehmenden

Weisungen zur rechtskonformen Verarbeitung zu erteilen.

3.2. Weisungen und rechtliche Verpflichtungen:

- Der Auftragnehmende verarbeitet die Daten des Auftraggebenden ausschließlich auf Basis

der erteilten Weisungen, sofern nicht gesetzliche Vorschriften der EU oder eines Mitgliedstaats eine andere Verarbeitung verlangen. Sollten solche gesetzlichen Anforderungen bestehen, wird der Auftragnehmende den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.

3.3. Entscheidungsbefugnis über Datenverarbeitung:

- Der Auftraggebende hat das Recht und die Pflicht, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden.

3.4. Kostenübernahme für zusätzliche Weisungen:

- Sollten zusätzliche Weisungen des Auftraggebenden über den im Hauptvertrag vereinbarten Umfang hinausgehen, trägt der Auftraggebende die dadurch entstehenden Kosten.

4. DIE RECHTE UND PFLICHTEN DES AUFTRAGNEHMENDEN

4.1. Dokumentierte Weisungen:

- Die dokumentierten Weisungen des Auftraggebenden sind Bestandteil dieses AVV.

4.2. Einhaltung des AVV und des Hauptvertrags:

- Der Auftragnehmende stellt sicher, dass die Datenverarbeitung im Rahmen des Hauptvertrags und gemäß den Bestimmungen dieses AVV erfolgt.

4.3. Mitteilung bei rechtlichen Bedenken:

- Im Falle einer Situation, in der die vom Auftraggebenden erteilten Weisungen in einem Konflikt stehen, ist eine Kommunikation erforderlich.

4.4. Unterstützung des Auftraggebenden:

- Der Auftragnehmende unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und angemessen ist. Hierzu gehören Transparenz in der Datenverarbeitung, Löschung von Daten auf Anfrage und die Bereitstellung von Informationen an betroffene Personen.

4.5. Zusammenarbeit bei Anfragen betroffener Personen:

- Sollte eine betroffene Person sich direkt an den Auftragnehmenden wenden, informiert dieser den Auftraggebenden und leitet die Anfrage weiter. Der Auftragnehmende interagiert

nicht direkt mit der betroffenen Person.

4.6. Ausnahmen von der Unterstützung:

- Nicht inbegriffen in der Unterstützung sind Prüfungen durch Dritte oder zusätzliche Zertifizierungen, die vom Auftraggebenden angefordert werden. Die Bestimmungen von Ziffer 10 bleiben hiervon unberührt.

5. VERTRAULICHKEIT

5.1. Zugriffsberechtigung:

- Zugang zu personenbezogenen Daten wird nur Personen gewährt, die diese für die Erfüllung ihrer Aufgaben im Rahmen des Vertrags benötigen.

5.2. Geheimhaltungspflicht:

- Der Auftragnehmende stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind.

6. SICHERHEIT DER VERARBEITUNG

6.1. Technische und organisatorische Maßnahmen:

- Der Auftragnehmende verpflichtet sich, angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die spezifischen Maßnahmen sind in Anhang A aufgeführt.

6.2. Anpassung der Sicherheitsmaßnahmen:

- Der Auftragnehmende darf Sicherheitsmaßnahmen ändern oder anpassen, sofern diese Änderungen das Sicherheitsniveau nicht mindern. Alle wesentlichen Änderungen müssen dokumentiert und vom Auftraggebenden genehmigt werden.

7. EINSATZ VON UNTERAUFTRAGNEHMENDEN

7.1. Anforderungen an Unterauftragnehmende:

- Der Auftragnehmende muss die Anforderungen gemäß Artikel 28 Absätze 2 und 4 DSGVO erfüllen, um Unterauftragnehmende zu beauftragen.

7.2. Verantwortlichkeit gegenüber dem Auftraggebenden:

- Der Auftragnehmende bleibt gegenüber dem Auftraggebenden für die Einhaltung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmenden verantwortlich.

7.3. Haftung bei Verstößen von Unterauftragnehmenden:

- Kommt ein Unterauftragnehmender seinen Datenschutzpflichten nicht nach, bleibt der Auftragnehmende gegenüber dem Auftraggebenden voll verantwortlich.

7.4. Datenschutzgarantien in Drittländern:

- Bei der Beauftragung von Unterauftragnehmenden in Drittländern stellt der Auftragnehmende sicher, dass diese ein angemessenes Datenschutzniveau bieten, beispielsweise durch EU-Standarddatenschutzklauseln.

8. BENACHRICHTIGUNG BEI VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

8.1. Benachrichtigungspflicht:

- Bei einer Datenschutzverletzung im Bereich des Auftragnehmenden oder eines Unterauftragnehmenden, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmende den Auftraggebenden unverzüglich.

8.2. Unterstützung bei gesetzlichen Meldepflichten:

- Der Auftragnehmende unterstützt den Auftraggebenden bei der Meldung solcher Vorfälle an die zuständigen Aufsichtsbehörden, unter Berücksichtigung der Art der Verarbeitung und
der verfügbaren Informationen.

8.3. Maßnahmen nach einer Datenverletzung:

- Der Auftragnehmende ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggebenden über diese Maßnahmen und eventuelle weitere Anweisungen.

9. LÖSCHEN UND RÜCKGABE VON DATEN

9.1. Rückgabe oder Löschung nach Beendigung:

- Bei Beendigung der Verarbeitungsdienste ist der Auftragnehmende verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggebenden zurückzugeben und

vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

9.2. Kosten für Rückgabe oder Löschung:
- Kosten, die im Zusammenhang mit der Rückgabe oder Löschung personenbezogener Daten entstehen, trägt der Auftraggebende.

10. INSPEKTION UND PRÜFUNG

10.1. Zugang zu Informationen und Auditierung:
- Der Auftragnehmende stellt dem Auftraggebenden alle erforderlichen Informationen zur Verfügung, um die Einhaltung der Anforderungen von Artikel 28 DSGVO und dieses AVV zu demonstrieren.

10.2. Zugang für Aufsichtsbehörden:
- Der Auftragnehmende gewährt den Aufsichtsbehörden, die gemäß geltendem Recht Zugang zu den Einrichtungen des Auftraggebenden und des Auftragnehmenden haben, oder deren Vertretern den erforderlichen Zugang zu seinen physischen Einrichtungen.

11. AUFTRAGGEBENDE UND AUFTRAGNEHMENDE

11.1. Kontaktinformationen:
- Die Parteien können wie folgt kontaktiert werden:
- Für den Auftraggebenden: [E-Mail-Adresse]
- Für den Auftragnehmenden: [E-Mail-Adresse]

11.2. Mitteilungspflicht bei Kontaktänderungen:
- Beide Parteien sind verpflichtet, sich gegenseitig über Änderungen in den Kontaktinformationen zu informieren.

12. BEGINN UND KÜNDIGUNG

12.1. Inkrafttreten des AVV:

- Dieser AVV tritt am Tag der Unterzeichnung durch beide Parteien in Kraft.

12.2. Recht auf Neuverhandlung:

- Beide Parteien haben das Recht, eine Neuverhandlung dieses AVV zu verlangen, wenn Gesetzesänderungen oder die Unzweckmäßigkeit der Bestimmungen eine solche Neuverhandlung erfordern.

12.3. Kündigungsbedingungen:

- Dieser AVV kann gemäß den Bedingungen des Rahmenvertrags gekündigt werden.

13. GELTENDES RECHT

13.1. Anwendbares Recht:

- Sofern im Rahmenvertrag nicht anders vereinbart, unterliegt dieser AVV dem deutschen Recht.

14. SONSTIGES

14.1. Aufbewahrung des AVV:

- Dieser AVV und alle Anhänge werden in Textform sowie elektronisch von beiden Parteien aufbewahrt.

14.2. Abhängigkeit von Rahmenvertrag:

- Dieser AVV und der Rahmenvertrag sind miteinander verbunden und können nicht separat gekündigt werden. Eine Ersetzung dieses AVV durch einen alternativen gültigen AVV ist ohne Kündigung des Rahmenvertrags möglich.

14.3. Vorrang des AVV:

- Dieser AVV hat Vorrang vor ähnlichen Bestimmungen in anderen Vereinbarungen zwischen den Parteien, einschließlich des Rahmenvertrags.

14.4. Dokumentation individueller Weisungen:

- Individuelle Weisungen nach Abschluss dieses AVV bedürfen der Textform und sind von beiden Parteien zu dokumentieren.

14.5. Freistellung von weiteren Verpflichtungen:

- Dieser AVV befreit den Auftragnehmenden nicht von Verpflichtungen, die ihm gemäß der DSGVO oder anderen Rechtsvorschriften obliegen.

14.6. Ausschluss des Zurückbehaltungsrechts:

- Ein Zurückbehaltungsrecht im Sinne des § 273 BGB hinsichtlich der für den Auftraggebenden verarbeiteten Daten wird hiermit ausgeschlossen.

14.7. Durchsetzbarkeit einzelner Bestimmungen:

- Sollte eine Bestimmung dieses Vertrags nicht durchsetzbar sein, so wird die Durchsetzbarkeit der übrigen Bestimmungen hierdurch nicht berührt.

15. UNTERSCHRIFTEN

Im Namen des Auftraggebenden: _____ [Unterschrift]

Im Namen des Auftragnehmenden: _____ [Unterschrift]

[Datum]

ANHANG A: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Risikobasierter Ansatz:

Der Auftragsnehmer kategorisiert Systeme nach Risikostufen, um das erforderliche Sicherheitsniveau zu verwalten und zu kontrollieren.

Geringes Risiko: Basisdaten wie Namen, E-Mail-Adressen und Websites. Erfordert Standard-Sicherheits- und Datenschutz-Compliance.

Hohes Risiko: Sensible Daten wie Passwörter, Gesundheitsdaten, Kreditkarteninformationen, Bankdaten und Angaben zur sexuellen Orientierung. Erfordert

erhöhte Sicherheitsmaßnahmen, Personaltraining, Datenschutz, Zugangskontrolle und Überwachung.

2. Maßnahmen von Unterprozessoren:

Die entsprechende Datenverarbeitung erfolgt auf IT-Systemen, die von Unterauftragnehmern betrieben werden.

3. Maßnahmen von Auftragsnehmer:

3.1 Geheimhaltung und Verschlüsselung:

Physischer Zugriff auf Datenverarbeitungsgeräte:

- Betrieb in externen Rechenzentren (Hosting) und bei externen Diensten (Software-as-a-Service) mit Zugangskontrolle.

- Büro des Auftragsnehmers:
- Eingangstüren stets verschlossen.
- Individuelle Zugangsberechtigung und Alarmanlage.
- Verwendung von Datenverarbeitungsgeräten:

- Zugriff auf extern gehostete/betriebene IT-Systeme mit besonderen Sicherheitsvorkehrungen (Verschlüsselung, VPN).

- Netzwerkabschottung durch Firewall.
- Zugang zu IT-Systemen nur mit Benutzerkennung und Passwort.
- Zwei-Faktor-Authentifizierung, sofern verfügbar.
- Dokumentierte Zutrittsberechtigungen.
- Bildschirmsperren an Arbeitsplätzen.

3.2 Integrität:

Weitergabekontrolle:

- Kein Zugang für Besucher zum Firmen-LAN/WLAN.
- Einsatz elektronischer Signaturen.
- Sichere Speicherung und Verarbeitung in Rechenzentren.
- Gesicherte Client-Server-Verbindungen (Verschlüsselung, VPN).
- Dokumentation von Datenübermittlungen.
- Eingabekontrolle:

- Protokollierung von Dateneingaben, Änderungen und Löschungen.
- Protokollierung von Zugangsversuchen.
- Überwachung von Systemadministratoren und Benutzeraktivitäten.
- Sicherung der Protokolldaten.

4. Verfügbarkeit und Belastbarkeit:

- Datensicherheitskonzepte gegen zufällige Zerstörung oder Verlust.
- Malware-Schutz und regelmäßiges Einspielen von Sicherheitsupdates.

5. Verfahren zur regelmäßigen Überprüfung und Bewertung:

Auftragskontrolle:

- Sorgfältige Auswahl der Auftragnehmer.
- Klare vertragliche Regelungen zur Datenverarbeitung.
- Formalisiertes Instruktionsmanagement.
- Schriftliche Erteilung von Weisungen.

- Kontrolle durch Geschäftsführung oder Datenschutzbeauftragten.

- Datenschutz-Management:
- Bestellung eines qualifizierten Datenschutzbeauftragten.
- Dokumentiertes Datenschutzmanagementsystem.

- Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter im

Datenschutz.