

a product by



# cara28

by



Date: 29.02.2024  
caralegal GmbH

---

## Executive Summary

- The contract does not regulate the need for approval of the use of further sub-processors.

- Suggested wording:

- *The controller authorizes the processor to use further sub-processors in accordance with the following paragraphs of this agreement.*

*General consent: The processor informs the controller about the use of new sub-processors. The controller may object to the use within a period of x days.*

*Separate consent: The involvement of subcontractors requires the prior written consent of the controller, which may be revoked at any time, and inclusion in Appendix B (list of subcontractors as additional processors). The controller is entitled to refuse consent at its own discretion.*

- There is no provision which stipulates that the processor must impose the same data privacy obligations on its subcontractors to which it is itself subject according to this contract. However, such a provision is embedded in Art. 28 para. 4 sentence 1 GDPR and therefore must urgently be included in the contract.

- Suggested wording:

- *The processor shall impose these same data privacy obligations on the subcontractors used as regulated in this contract.*

- The obligation of the processor to support the controller with inquiries from data subjects as per Art. 12-22 GDPR is not specified in the contract.

- Suggested wording:

- *The processor supports the controller in fulfilling the rights of data subjects as per Art. 12 to 22 GDPR.*

- There is no provision which stipulates that the controller can verify the processor's compliance with the requirements of Art. 28 GDPR.

-

Suggested wording:

- The processor shall ensure that the controller is able to verify compliance with the processor's obligations as per Art. 28 GDPR and shall provide all information necessary to demonstrate compliance with the obligations set out in this article.*
- The contract regulates that instructions are generally subject to costs. Such a provision is inadmissible, as the contractor cannot waive certain obligations with respect to the controller.

Only a provision stating that instructions that exceed the contractual agreements and are not necessary to rectify or prevent infringements by the contractor are subject to a charge.

## Clauses that could prevent the conclusion of the contract:

The contract does not regulate the need for approval of the use of further sub-processors.

○ Suggested wording:

○ *The controller authorizes the processor to use further sub-processors in accordance with the following paragraphs of this agreement.*

*General consent: The processor informs the controller about the use of new sub-processors. The controller may object to the use within a period of x days.*

*Separate consent: The involvement of subcontractors requires the prior written consent of the controller, which may be revoked at any time, and inclusion in Appendix B (list of subcontractors as additional processors). The controller is entitled to refuse consent at its own discretion.*

○ Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.

There is no provision which stipulates that the processor must impose the same data privacy obligations on its subcontractors to which it is itself subject according to this contract. However, such a provision is embedded in Art. 28 para. 4 sentence 1 GDPR and therefore must urgently be included in the contract.

○ Suggested wording:

○ *The processor shall impose these same data privacy obligations on the subcontractors used as regulated in this contract.*

The obligation of the processor to support the controller with inquiries from data subjects as per Art. 12-22 GDPR is not specified in the contract.

○ Suggested wording:

○ *The processor supports the controller in fulfilling the rights of data subjects as per Art. 12 to 22 GDPR.*

○

**Marked 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 Auftragnehmer stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmer 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 Auftragnehmer ergreift unverzüglich Maßnahmen, um die Daten zu sichern und potenziell negative Folgen für die betroffenen Personen zu minimieren, und informiert den Auftraggeber 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 Auftragnehmer verpflichtet, alle personenbezogenen Daten zu löschen oder an den Auftraggeber zurückzugeben und vorhandene Kopien zu vernichten, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der Daten vor.

There is no provision which stipulates that the controller can verify the processor's compliance with the requirements of Art. 28 GDPR.

○ Suggested wording:

○ *The processor shall ensure that the controller is able to verify compliance with the processor's obligations as per Art. 28 GDPR and shall provide all information necessary to demonstrate compliance with the obligations set out in this article.*

○ Marked text:

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

The contract regulates that instructions are generally subject to costs. Such a provision is inadmissible, as the contractor cannot waive certain obligations with respect to the

controller.

Only a provision stating that instructions that exceed the contractual agreements and are not necessary to rectify or prevent infringements by the contractor are subject to a charge.

- **Marked 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 Auftragnehmer 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 Auftragnehmer unterstützt den Auftraggebenden bei der Einhaltung der Pflichten gemäß den Artikeln der DSGVO, soweit dies technisch und organisatorisch machbar und

---

## Clauses that require your attention:

- No list of subcontractors is attached to the contract. The inclusion of a list of subcontractors with their address, legal form and a brief description of their tasks is not absolutely necessary in order to conclude the contract, but it is recommended for the purposes of clarity and transparency. If there is only a link provided to this list, we recommend that the list is downloaded and filed in order to be able to comply with in-house verification obligations.

- **Suggested wording:**

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

- **Marked 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 quali-

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

- The contract contains measures for the regular evaluation and review of the TOM used. Please check the appropriateness of the measures for the specific data processing.

- Marked 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.

- The measures for pseudonymization are not sufficiently included in the contract. Although pseudonymization is listed as a possible measure in Art. 32 GDPR, it is not mandatory. With regard to the specific measures, the processor can in fact be granted a certain degree of flexibility within the scope of appropriateness. If some of the measures listed in Art. 32 GDPR are missing in this contract, this does not prevent the conclusion of the contract.

- Marked 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 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 Benutzererkennung 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:

The contract contains measures to protect the integrity of the data. Please check the appropriateness of the measures for the specific data processing.

○ Marked 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 Benutzererkennung und Passwort. - Zwei-Faktor-Authentifizierung, sofern verfügbar. - Dokumentierte Zutrittsberechtigungen. - Bildschirmsperren an Arbeitsplätzen. 3.2 Integrität: Weitergabekontrolle: - Kein Zu-



gang 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.

- The contract does not contain a provision on the use of sub-processors.
  - Suggested wording:
    - *The use of sub-processors requires provisions to be made on the permissibility of their use, including the requirement to disclose their use to the controller and the imposition of the same data privacy obligations of the contract on the sub-processors.*
    - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- The contract does not contain a provision for the processing of special categories of personal data. Please ensure that the data processing does not actually include any special categories of personal data.
  - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- The contract contains a list of the groups of data subjects affected by the data processing. Please ensure that the specified data is complete.
  - Marked 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 und 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 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.

- The text of the contract makes no provision regarding the use of data for internal purposes. Consequently, the use of the data for internal purposes is prohibited.
  - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- The location of the data processing is not regulated. This is particularly recommended so that the safeguards for data processing can be adapted accordingly.
  - Suggested wording:
    - *The processing and use of the data shall take place solely in the European Union.*

- Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- The contract contains categories of data subjects affected by the data processing. Please ensure that the specified categories are complete.

- Marked 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 Auftragnehmer 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 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 Auftragnehmer Weisungen zur rechtskonformen Verarbeitung zu erteilen. 3.2. Weisungen und rechtliche Verpflichtungen: - Der Auftragnehmer 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 Auftragnehmer den Auftraggebenden darüber informieren, sofern dies gesetzlich zulässig ist.

- The contract contains measures to ensure the resilience of the systems. Please check the appropriateness of the measures for the specific data processing.

- Marked text:

Überwachung. 2. Maßnahmen von Unterverarbeitern: 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.

The contract contains measures to protect the confidentiality of the data. Please check the appropriateness of the measures for the specific data processing.

○ Marked 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 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 Benutzererkennung 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.

The contract contains measures for the encryption of data. Please check the appropriateness of the measures for the specific data processing.

○ Marked text:

1. Risikobasierter Ansatz: Der Auftragnehmer 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 Auftragnehmer: 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 Auftragnehmers: - 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 Benutzererkennung 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 (Verschlüs-

selung, 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.

- The contract contains measures to guarantee the availability of the systems. Please check the appropriateness of the measures for the specific data processing.

- **Marked 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.

The exception to the statutory disclosure requirement is not specified in the contract. This is provided for in Art. 28 para. 3 sentence 2 lit. a GDPR.

○ Suggested wording:

○ *A disclosure requirement explicitly does not exist if such notification is prohibited by existing law due to important grounds of public interest, cf. Art. 28 para. 3 sentence 2 lit. a GDPR.*

○ Marked 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 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.

---

## Clauses you can be reassured about

The subject matter of the processing is described in sufficient detail.

○ Marked text:

AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmender: [Name des Auftragnehmenden] INHALTSVERZEICHNIS Gegenstand, Dauer, Art und Zweck der Verarbeitung Art der personenbezo-

genen 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 Auftragnehmende 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 und 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 Verarbeitung. 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

The duration of the processing is regulated to a sufficiently specific degree.

○ Marked text:

AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmer: [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 Auftragnehmer 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 Auftragnehmer im Auftrag des Auftraggebenden. 1.2. Verarbeitung im Auftrag: - Der Auftragnehmer 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 Auftragnehmer 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 Arbeitsort sowie freiwillig geteilte Benutzerprofile verarbeitet werden. 2.3. Kategorien von betroffenen Personen: - Betroffen sind Mitarbeiter und Administratoren der Plattform des Auftraggebenden.

den, 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. 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

- The contract contains a provision stipulating that the data processing may only be conducted according to the instructions of the controller.

This clause is of great importance as it defines the clear allocation of responsibility with regard to data processing. It ensures that the processor may only process the personal data within the scope of the explicit instructions of the controller.

- Marked 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 Daten-

verarbeitung 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 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

The contract does not contain a liability provision, consequently general liability as per Art. 82 GDPR applies.

The contract does not contain any other clauses that involve unreasonable risks for the controller.

- The contract does not exclude any services from the concept of data processing across the board.
- The nature and purpose of the data processing are described in sufficient detail.
  - Marked text:

AUFTRAGSVERARBEITUNGSVERTRAG Zwischen: Auftraggebender: [Name des Auftraggebenden] Auftragnehmer: [Name des Auftragnehmers] INHALTSVERZEICHNIS Gegenstand, Dauer, Art und Zweck der Verarbeitung Art der personenbezogenen Daten Rechte und Pflichten des Auftraggebenden Die Rechte und Pflichten des Auftragnehmers Vertraulichkeit Sicherheit der Verarbeitung Einsatz von Unterauftragnehmern Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Löschen und Rückgabe von Daten Inspektion und Prüfung Auftraggebende und Auftragnehmer 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 Auftragnehmer im Auftrag des Auftraggebenden. 1.2. Verarbeitung im Auftrag: - Der Auftragnehmer 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 Auftragnehmer 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 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

- The processor undertakes to assist in the notification of the data subject(s) as per Art. 34 GDPR.

- Marked 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 Auftragnehmer stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind. 6. SICHERHEIT DER VERARBEITUNG 6.1. Technische und organisatorische Maßnahmen: - Der Auftragnehmer 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 Auftragnehmers oder eines Unterauftragnehmers, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmer den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmer 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 Auftragnehmer 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 Auftragnehmer 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.

- A list of the TOMs implemented is attached to the contract.

- Marked text:

1. Risikobasierter Ansatz: Der Auftragnehmer 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 Auftragnehmer: 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.

- There are no contractual provisions regarding processing outside the EU/EEA by the processor itself.
  - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- The processor undertakes to assist in reporting data privacy incidents to the relevant authority as per Art. 33 GDPR.
  - Marked text:

DATEN 8.1. Benachrichtigungspflicht: - Bei einer Datenschutzverletzung im Bereich des Auftragnehmers oder eines Unterauftragnehmers, die zu einem Risiko für die personenbezogenen Daten führen könnte, informiert der Auftragnehmer den Auftraggebenden unverzüglich. 8.2. Unterstützung bei gesetzlichen Meldepflichten: - Der Auftragnehmer 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 Auftragnehmer 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.

The processor is obliged to delete or return the data following completion of the processing services.

○ Marked 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. 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

- The processor undertakes to support the security of processing as per Art. 32 GDPR.

- Marked 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.

- The processor undertakes to ensure the security of the processing by implementing appropriate technical and organizational measures in accordance with Art. 32 GDPR.

- Marked 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 Einhaltung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmenden verantwortlich.

**Deadlines are included for the support measures.**

**Marked 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.

- The contract contains a provision according to which instructions must be documented.

This is an extremely important step for ensuring transparency and traceability with regard to data processing.

- Marked 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 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 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. 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.

## Clauses that could not be clearly assigned:

- cara28 was unable to determine whether the contract contains a remuneration provision to support the processor in the measures pursuant to Art. 32 to 36 GDPR.
  - Suggested wording:
    - *The processor supports the controller in fulfilling the obligations as per Art. 32 to 36 GDPR.*
    - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- cara28 was unable to determine whether the processor undertakes to subject its employees to confidentiality.
  - Suggested wording:
    - *During execution, the processor only uses employees who have been obliged to maintain confidentiality and who have been familiarized with the relevant data privacy provisions. The obligation to maintain confidentiality continues to apply even after completion of the contract.*
    - Marked text:

6.2. Anpassung der Sicherheitsmaßnahmen: - Der Auftragnehmer 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 Unterauftragnehmer: - Der Auftragnehmer muss die Anforderungen gemäß Artikel 28 Absätze 2 und 4 DSGVO erfüllen, um Unterauftragnehmer zu beauftragen. 7.2. Verantwortlichkeit gegenüber dem Auftraggebenden: - Der Auftragnehmer bleibt gegenüber dem Auftraggebenden für die Einhaltung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmer verantwortlich.
- cara28 was unable to determine whether the contract covers all processing of personal data over time.

- Suggested wording:
  - *The commitment to privacy and the obligation to maintain secrecy regarding business secrets shall continue to apply beyond the term of the contract.*
- Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- cara28 was unable to determine whether the contract contains a provision on remote working.
  - Marked text: A corresponding clause is not included in the contract, therefore no text passage has been marked.
- cara28 was unable to determine whether the contract contains a provision according to which the processor provides the controller with all necessary information to demonstrate compliance with the obligations set out in Art. 28 GDPR.
  - Suggested wording:
    - *The processor provides the controller with all information necessary to demonstrate compliance with the obligations stipulated in Art. 28 GDPR.*
  - Marked 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 Auftragnehmer wenden, informiert dieser den Auftraggeber und leitet die Anfrage weiter. Der Auftragnehmer 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 Auftraggeber angefordert werden. 11.1. Kontaktinformationen: - Die Parteien können wie folgt kontaktiert werden: - Für den Auftraggeber: [E-Mail-Adresse] - Für den Auftragnehmer: [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 was unable to determine whether the contract contains a provision according to which a notification must be made to the controller prior to processing in the event of a legally prescribed deviation from the instruction.

○ Suggested wording:

○ *The contractor processes the data in accordance with the controller's instructions, unless it is obliged to do so by statute or other contractual agreements.*

○ Marked 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 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

cara28 was unable to determine whether the contract contains an obligation for the processor to point out allegedly unlawful instructions. (Art. 28 para. 3 GDPR)

- Suggested wording:
  - *If the processor considers the instruction to be unlawful, it informs the controller immediately.*
- Marked 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

## Source Document

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

### 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 Auftragnehmende

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 und Job-Titel. Zudem können Hintergrundinformationen wie Organisationseinheit und Arbeitssort

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 Auftragnehmer 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 Auftragnehmer wenden, informiert dieser den Auftraggebenden und leitet die Anfrage weiter. Der Auftragnehmer 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 Auftragnehmer stellt sicher, dass alle Personen zur gesetzlichen Geheimhaltung verpflichtet sind.

### 6. SICHERHEIT DER VERARBEITUNG

#### 6.1. Technische und organisatorische Maßnahmen:

- Der Auftragnehmer 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 Auftragnehmer 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 Unterauftragnehmer:

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

#### 7.2. Verantwortlichkeit gegenüber dem Auftraggebenden:

- Der Auftragnehmer bleibt gegenüber dem Auftraggebenden für die Einhaltung der datenschutzrechtlichen Pflichten durch die Unterauftragnehmer verantwortlich.

#### 7.3. Haftung bei Verstößen von Unterauftragnehmern:

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

#### 7.4. Datenschutzgarantien in Drittländern:

- Bei der Beauftragung von Unterauftragnehmern in Drittländern stellt der Auftragnehmer 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 Auftragnehmern 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 Auftragnehmer gewährt den Aufsichtsbehörden, die gemäß geltendem Recht Zugang zu den Einrichtungen des Auftraggebenden und des Auftragnehmers 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 Auftragnehmer: [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 Auftragnehmer 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 Auftragnehmer:

#### 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.