Anlage: Vereinbarung zur Auftragsverarbeitung nach Artikel 28 DS-GVO

Präambel

Diese Anlage dient der konkreten Umsetzung der datenschutzrechtlichen Verpflichtungen von Auftragnehmer und Auftraggeber, die sich aus den gesetzlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) im Rahmen der Auftragsverarbeitung (Artikel 28 DS-GVO) in Bezug auf den zwischen den Parteien abgeschlossenen und ihrem Verhältnis zugrundeliegenden Vertrag („Hauptvertrag") ergeben.

1. Anwendungsbereich

Der Anwendungsbereich dieser Anlage umfasst alle Tätigkeiten, bei denen der Auftragnehmer, seine Mitarbeiter oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers oder seinerseitiger Auftraggeber in Berührung kommen und hierbei Weisungen des Auftraggebers umsetzen sollen („Auftragsverarbeitung“). Hierzu zählt auch die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen des Auftraggebers durch den Auftragnehmer, soweit dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
Eine „Weisung“ im Sinne dieser Anlage ist insbesondere eine auf Grund des zugrundeliegenden Hauptvertrages ergehende Anordnung des Auftraggebers an den Auftragnehmer im Sinne des Artikel 29 DS-GVO personenbezogene Daten des Auftraggebers bzw. dessen Auftraggebers gemäß Artikel 4 Nr. 2 DS-GVO auf datenschutzrelevante Weise zu verarbeiten, insbesondere sie zu erheben, zu erfassen, zu organisieren zu ordnen, zu speichern, anzupassen oder zu verändern, auszulesen, abzufragen, zu verwenden, durch Offenlegung zu übermitteln, zu verbreiten oder auf andere Weise bereitzustellen, abzugleichen, zu verknüpfen, einzuschränken, zu sperren, zu löschen oder zu vernichten. Unerheblich ist dabei, ob eine Weisung bereits im Hauptvertrag festgelegt ist oder zu einem späteren Zeitpunkt erteilt, ergänzt, geändert oder ersetzt wird.
„Personenbezogene“ Daten im Sinne dieser Anlage sind alle Informationen im Sinne des Artikel 4 Nr. 1 DS-GVO, die sich auf meine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Hierzu gehören insbesondere Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person.

2. Gegenstand der Auftragsverarbeitung; Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand des Auftrages ergibt sich aus dem Hauptvertrag bzw. seiner Leistungsbeschreibung nebst Anlagen.

2.2 Der Auftragnehmer verarbeitet die personenbezogenen Daten, die ihm im Rahmen der Erfüllung seiner Verpflichtung aus dem zugrundeliegenden Hauptvertrag zugänglich gewordenen sind, ausschließlich nach Weisungen des Auftraggebers.

2.3 Der Umfang, die Art und der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber, ergeben sich aus dem Hauptvertrag nebst Anlagen.
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen

2.4 Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist zuvorderst der Auftraggeber verantwortlich. Der Auftraggeber ist insbesondere für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze so auch für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich d.h. er ist „Verantwortlicher" im Sinne des Artikel 4 Nr. 7 DS-GVO. Er behält sich insoweit hinsichtlich der Verarbeitung im Auftrag gegenüber

dem Auftragnehmer ein umfassendes Weisungsrecht vor.

2.5 Die Vergütung für die Auftragsverarbeitung bestimmt sich nach dem Hauptvertrag.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 — 36 der DS-GVO genannten Pflichten zur Sicherstellung der Sicherheit personenbezogener Daten, in Bezug auf Meldepflichten bei Datenpannen, der Erstellung von Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

3.2 Der Auftragnehmer ist verpflichtet, personenbezogene Daten, die ihm auf der Grundlage des mit dem Auftraggeber geschlossenen Hauptvertrages zugänglich werden, ausschließlich im Rahmen der getroffenen Weisungen des Auftraggebers zu verarbeiten. Der Auftragnehmer darf die Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten (Artikel 29 DS-GVO) außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3a) DS-GVO vor.
Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
Kopien der erhobenen oder zur Datenverarbeitung überlassenen Daten werden nicht erstellt. Hiervon ausgenommen sind Sicherungskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung Der Auftragnehmer hat personenbezogene Daten zu berichtigen zu löschen oder zu sperren, wenn der Auftraggeber ihn hierzu anweist.

3.3 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im, bzw. gehen in das Eigentum des Auftraggebers über. Sie werden besonders gekennzeichnet und unterliegen der laufenden — automatisierten —Verwaltung. Ein- und Ausgang werden dokumentiert. Der Auftragnehmer wird diese so sorgfältig verwahren, dass sie Dritten nicht zugänglich sind.

3.4 Der Auftragnehmer wird gemäß Artikel 32 DS-GVO zur ordnungsgemäßen Erfüllung seiner vertraglichen Verpflichtungen im Rahmen der Auftragsverarbeitung unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen insbesondere seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht und ein angemessenes Schutzniveau erreicht wird. Er wird sich hierbei soweit möglich insbesondere auch der Pseudonymisierung und der Verschlüsselung personenbezogener Daten bedienen. Er wird ferner technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der Datenschutz-Grundverordnung (Artikel 28 Abs. 3 lit. c, Artikel 24, Artikel 32 DS-GVO insbesondere i.V.m. Artikel 5 Abs. 2 DS-GVO) genügen. Dies beinhaltet insbesondere:

3.4.1 Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

3.4.2 zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

3.4.3 zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

3.4.4 zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

3.4.5 zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

3.4.6 zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

3.4.7 zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind sowie bei physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (**Verfügbarkeitskontrolle**),

3.4.8 zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Der Auftragnehmer stellt insbesondere sicher, dass sie jederzeit von sonstigen Datenbeständen getrennt zu Verfügung gestellt werden können (**Trennungskontrolle**).

Der Auftragnehmer stellt sicher, dass über ein von ihm implementiertes Verfahren die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit sowie die Nachweisbarkeit der vorstehend aufgeführten technischen und organisatorischen Maßnahmen gewährleistet ist. In Bezug auf die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann der Auftragnehmer auf von ihm vorgelegte, höchstens drei Jahre alte Zertifizierungen nach Artikel 42 DS—GVO verweisen, deren Einhaltung in angemessenen Zeiträumen geprüft und bestätigt wurde.

3.5 Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Er stellt ferner sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß Artikel 29 DS-GVO diese Daten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland zur Verarbeitung verpflichtet sind, ausschließlich auf Weisung des Verantwortlichen verarbeiten und in die Schutzbestimmungen der Datenschutz-Grundverordnung eingewiesen worden sind.
Die Auftragsverarbeitung in Privatwohnungen ist nur mit vorheriger Zustimmung des Auftraggebers und nur im Einzelfall gestattet. Vor der Einrichtung eines Tele-Heimarbeitsplatzes ist zu prüfen, ob die Verarbeitung personenbezogener Daten zwingend erforderlich ist oder ob eine Verarbeitung von Vorgängen auch ohne Personenbezug oder in pseudonymisierter Form möglich ist. Soweit die Auftragsverarbeitung in einer Privatwohnung erfolgt, stellt der Auftragnehmer sicher, dass die bestehenden Kontrollrechte des Auftraggebers durch diesen im vollen Umfang ausgeübt werden können.

3.6 Der Auftragnehmer benennt dem Auftraggeber gegenüber unverzüglich nach Unterzeichnung des zugrundeliegenden Hauptvertrages den Datenschutzbeauftragten, der seine Tätigkeit gem. Artikel 38 und 39 DS-GVO ausübt Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der Kontaktaufnahme mitgeteilt. Jeder Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

3.7 Der Auftragnehmer übergibt dem Auftraggeber auf dessen Anforderung das gemäß Artikel 30 Abs. 2 DS-GVO von ihm hinsichtlich seiner beauftragten Verarbeitungstätigkeiten zu führende Verarbeitungsverzeichnis und stellt dieses auf Anfrage der Aufsichtsbehörde zur Verfügung.

3.8 Der Auftragnehmer unterrichtet den Auftraggeber ferner unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder über andere datenschutzrelevante Unregelmäßigkeiten bei der Verarbeitung der Daten.

3.9 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer dem Auftraggeber auf dessen schriftliche Anforderung sämtliche in seinen Besitz gelangten Unterlagen, die im Zusammenhang mit dem Auftragsverhältnis stehen auszuhändigen. Datenträger, die Daten des Auftraggebers als „verantwortliche Stelle“ beinhalten, sind hinsichtlich der betreffenden Daten insoweit physisch zu löschen. Die Löschung ist dem Auftraggeber schriftlich zu bestätigen.
Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, die auf Einzelanweisungen beruhen, welche über den vertraglich vereinbarten Leistungsumfang hinausgehen sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist für die rechtliche Beurteilung der Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist verpflichtet Änderungen des zugrundeliegenden Hauptvertrages zur Auftragsverarbeitung soweit sie unter Artikel 28 DS-GVO fallen, schriftlich zu beauftragen. Änderungen von Weisungen über Art, Umfang und Verfahren der Datenverarbeitung, die sich im Rahmen des vertraglich Vereinbarten halten, sollen schriftlich erteilt werden; der Auftragnehmer ist berechtigt nicht schriftlich erteilte Weisungen zurückzuweisen

4.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich und umfassend, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt Entsprechendes gilt für den Fall einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO.

4.4 Der Auftraggeber behandelt, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen insbesondere im Hinblick auf Datensicherungsmaßnahmen des Auftragnehmers vertraulich.

5. Zusammenarbeit von Auftraggeber und Auftragnehmer

5.1 Der Auftragnehmer und der Auftraggeber arbeiten auf entsprechende Anfrage der Aufsichtsbehörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche der betroffenen Personen gern. Kapitel III der DS—GVO (sh auch Ziffer 7) sowie bei der Einhaltung der in Artikel 33 — 36 DS-GVO genannten Pflichten.

5.2 Der Auftragnehmer verpflichtet sich ferner:

5.2.1 den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den dieser Vereinbarung zugrundeliegenden Auftrag beziehen, zu informieren,

5.2.2 den Auftraggeber, soweit er seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, nach besten Kräften zu unterstützen.

5.3 Auch bereits während der Laufzeit dieser Vereinbarung berichtigt löscht oder schränkt der Auftragnehmer die Verarbeitung von personenbezogenen Daten ein, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

5.4 Auftraggeber und Auftragnehmer benennen jeweils die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen im **Anhang** zu dieser Vereinbarung. Bei einem Wechsel oder einer sich abzeichnenden längerfristigen Verhinderung der benannten Personen, sind der jeweils anderen Partei Vertreter bzw. Nachfolger unverzüglich per Brief oder per Fax mitzuteilen.

5.5 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr einsprechender Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

6. Anfragen Betroffener an den Auftraggeber/den Auftragnehmer

6.1 Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung stellen.

6.2 Macht der Betroffene sein Recht auf Berichtigung, Löschung oder Sperrung seiner Daten geltend, nimmt der Auftragnehmer nur auf Weisung des Auftraggebers die Berichtigung, Sperrung oder Löschung vor oder leitet die Anfrage an den Auftraggeber weiter, soweit ihm die Vornahme der Anpassungen nicht möglich oder vertraglich nicht erlaubt ist.

6.3 Wendet sich die betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter und unterstützt den Auftraggeber nach dessen Weisungen im Rahmen seiner Möglichkeiten.

6.4 Der Auftraggeber ist verpflichtet dem Auftragnehmer die diesem durch Maßnahmen nach Ziff. 7.1 bis 7.3 entstehenden Kosten gemäß der zwischen den Parteien im zugrundeliegenden Hauptvertrag getroffenen generellen Kostenregelungen zu ersetzen.

7. Unterauftragsverhältnisse

7.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung des Auftragsgegenstandes respektive die Leistungspflichten beziehen. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Leistungspflichten verbundene Unternehmen des Auftragnehmers i.S.d. § 15 AktG zur Leistungserfüllung heranzieht Die Beauftragung sonstiger dritter Unternehmen mit Leistungen aus dem Auftragsverhältnis bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers per Brief oder Fax.

7.2 Der Auftragnehmer stellt sicher, dass der Unterauftragnehmer gegenüber dem Auftragnehmer in entsprechender

Weise verpflichtet ist, wie der Auftragnehmer gegenüber dem Auftraggeber nach dieser Vereinbarung verpflichtet ist. Der Auftragnehmer hat die Einhaltung dieser Pflichten des Unterauftragnehmers regelmäßig zu überprüfen. Eine Weiterleitung von Daten von dem Auftragnehmer an den Unterauftragnehmer ist erst zulässig, wenn sichergestellt ist, dass der Unterauftragnehmer den datenschutzrechtlichen Verpflichtungen des Auftragnehmers vollumfänglich beigetreten ist.

7.3 Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber gegenüber dem Unterauftragnehmer die gleichen Kontrollrechte hat wie der Auftraggeber sie gegenüber dem Auftragnehmer selbst hat. Die vertragliche Absicherung ist so zu gestalten, dass sie den Auftraggeber — unbeschadet der Verantworlichkeit des Auftragnehmers für den Unterauftragnehmer — unmittelbar gegenüber dem Unterauftragnehmer berechtigt. Auf Anforderung ist der Auftragnehmer verpflichtet, dem Auftraggeber Auskunft über den für die Kontrollrechte wesentlichen Vertragsinhalt und über die Umsetzung der datenschutzrechtlichen Verpflichtungen durch den Unterauftragnehmer zu geben.

7.4 Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen insbesondere z.B. Telekommunikationsleistungen Post-/Transportdienstleistungen, Wartung und Benutzerservice Reinigungskräfte oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene Vereinbarungen zur Absicherung vor einem Missbrauch der Daten des Auftraggebers zu treffen sowie entsprechende Kontrollmaßnahmen zu ergreifen.

7.5 Der Einsatz von Unter-Unterauftragnehmern ist unzulässig. Der Auftragnehmer verpflichtet sich seinen Unterauftragnehmern vertraglich zu untersagen, ihrerseits weitere Unterauftragnehmer einzusetzen.

8. Kontrollrechte

8.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftraggeber hat ferner das Recht die Einhaltung der zwischen den Parteien vereinbarten datenschutzrechtlichen Regelungen und/oder der gesetzlichen Vorschriften zum Datenschutz, soweit diese durch das Vertragsverhältnis berührt sind, jederzeit im erforderlichen Umfang zu überprüfen. Er kann hierzu entweder:

8.1.1 eine Selbstauskunft des Auftragnehmers einholen, deren Bestandteil z.B. unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung, Zertifikate zu Datenschutz und/oder Informationssicherheit genehmigte Verhaltensregeln nach Artikel 40 DS-GVO oder Zertifikate nach Artikel 42 DS-GVO sind.

8.1.2 nach vorheriger Anmeldung und zu den üblichen Geschäftszeiten des Auftragnehmers sowie unter Berücksichtigung von dessen betrieblichen Belangen, die Sicherstellung der auf Grund dieser Vereinbarung für den Auftragnehmer bestehenden rechtlichen Verpflichtungen überprüfen. Er kann dabei insbesondere Einsicht in die vom Auftragnehmer für ihn erhobenen, verarbeiteten oder genutzten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

8.2 Der Auftraggeber ist berechtigt die Überprüfungen selbst durchzuführen oder durch einen beauftragten Dritten (Prüfer) durchführen lassen. Das Ergebnis der Kontrollen ist zu dokumentieren. Der Auftragnehmer ist entsprechend zur Mitwirkung verpflichtet. Er verpflichtet sich dem Auftraggeber bzw. dem Prüfer auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

8.3 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer keinen Vergütungsanspruch geltend machen.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.2 Nach Abschluss der vertraglich vereinbarten Tätigkeiten oder früher nach Aufforderung durch den Auftraggeber — spätestens mit Beendigung des Hauptvertrages — hat der Auftragnehmer sämtlich in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestande die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung

datenschutzgerecht zu vernichten. Gleiches gilt für den Auftrag betreffendes Test- und Ausschussmaterial Auf Aufforderung des Auftraggebers hat der Auftragnehmer ein Protokoll der Löschung vorzulegen.

9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende des Hauptvertrages hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende des Hauptvertrages dem Auftraggeber übergeben.

10. Haftung

10.1 Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Artikel 82 DS-GVO getroffenen Regelung.

10.2 Der Auftragnehmer haftet im Innenverhältnis ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

10.2.1 er den aus der DS-GVO resultierenden und speziell für den Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

10.2.2 er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder

10.2.3 er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

10.3 Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Sonstiges

11.1 Auftragnehmer und Auftraggeber bestimmen, soweit sich solches nicht schon aus dem zugrundeliegenden Hauptvertrag ergibt, unverzüglich nach Unterzeichnung des Vertrages einen fachkundigen Ansprechpartner, der während der Durchführung des Vertrages für die jeweilige Partei verbindliche Entscheidungen treffen kann und bei der Ausübung der bestehenden Kontrollrechte für die jeweils andere Partei zur Verfügung steht.

11.2 Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger für den Auftragnehmer ausgeschlossen.

11.3 Soweit die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme durch eine Insolvenz oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird ferner alle in diesem Zusammenhang tätig werdenden Personen oder Organisationen unverzüglich darüber informieren, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als Verantwortlichem iSd Artikels 4 Nr. 7 DS-GVO liegt.

11.4 Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des zugrundeliegenden Hauptvertrages.

11.5 Die Datenverarbeitung unter dieser Vereinbarung soll nur in Deutschland stattfinden. Eine Datenverarbeitung in Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, ist nach schriftlicher Bestätigung durch den Auftraggeber für den vereinbarten Einzelfall zulässig. Datenverarbeitungen in anderen Ländern (sog. Drittstaaten) sind grundsätzlich unzulässig. Entsprechendes gilt für jeglichen Zugriff auf die Daten durch den Auftragnehmer, z.B. im Rahmen interner Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

11.6 Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist der Sitz des Auftragnehmers.

11.7 Es gilt deutsches Recht.

_____	München, der 23.05.2018
Ort, Datum	**Ort, Datum**
	
_____	Günter Dallmayr - Geschäftsführung
Auftraggeber	**Auftragnehmer**

Anlage 1 - Auftragsspezifische Vereinbarungen

1. Gegenstand und Dauer der Auftragsverarbeitung

Bezüglich Gegenstand und Dauer der Auftragsverarbeitung wird auf dem oder den bestehenden Miet- und/oder Servicevertrag verwiesen.

2. Umfang, Art und Zweck der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

I. Umfang, Art und Zweck der Datenverarbeitung:

- Der Auftragnehmer erbringt Serviceleistungen in der Regel remote über das öffentliche Netzwerk. Der Auftragnehmer kann somit personenbezogene Daten einsehen von Mitarbeitern welchen eine Nebenstellenrufnummer zugeordnet ist.
- Der Auftragnehmer erbringt je nach Vertragsverhältnis des Weiteren zusätzliche IT Leistungen die sich aus dem aktuell laufenden Vertrag ergeben (leer wenn keine zusätzlichen Leistungen erbracht werden):
    - …….

II. Kreis der Betroffenen (Kategorien):

- Mitarbeiter des Kunden denen eine Nebenstellenrufnummer in der Telefonanlage am Standort zugewiesen ist.
- Je nach Vertrag (leer wenn keine zusätzlichen Leistungen erbracht werden):
    - ……..

III. Art der Daten (Kategorien):

- Name
- Vorname
- Abteilung
- Nebenstellenrufnummer
- Weiteres je nach Vertrag (leer wenn keine zusätzlichen Leistungen erbracht werden):
    - …….
    - …….
    - …….

3. Unterauftragsverhältnisse

Als Unterauftragnehmer werden derzeit seitens des Auftragnehmers folgende Unternehmen (Firma, Anschrift, im Rahmen der Auftragsverarbeitung wahrgenommene Tätigkeit) oder freien Mitarbeiter (Name, Anschrift, im Rahmen der Auftragsverarbeitung wahrgenommene Tätigkeit) eingesetzt (sofern sich Unterauftragnehmer in einem Drittstaat befinden, sind das Land sowie getroffene Maßnahmen, welche das angemessene Datenschutzniveau gewährleisten, aufzuführen):

- …….
- …….

4. Kontaktdaten des Datenschutzbeauftragten:

Als Datenschutzbeauftragter beim Auftragnehmer ist die folgende Person bestellt:

- Name: Claudia Mantl
- Organisationseinheit: Vertrieb
- Telefonnummer: +49 (89) 820 10 - 226
- E-Mail-Adresse: Claudia.Mantl@bvg-systemhaus.de

Anlage 2 - Technische und organisatorische Maßnahmen

I. Anmerkung:

- Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

- Alternativ kann auch ein durch den Auftragnehmer vorgelegtes und vom Auftraggeber akzeptiertes Sicherheitskonzept als Anlage 2 beigefügt werden, sofern dieses die Vorgaben von Art. 32 Abs. 1 DS-GVO angemessen umsetzt.

1. Vertraulichkeit und Zutrittskontrolle (Art. 32 Abs. 1 lit. b DS-GVO)

I. Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Der Zutritt zu den Räumlichkeiten der BVG Communication Technologies GmbH und den enthaltenen DV Anlagen ist nur via Schloss/Schlüssel möglich

II. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Ein Zugangsschutz (mind. Benutzer/Passwort) zu DV Anlagen mit regelmäßiger Änderung der Passwörter ist eingerichtet
- Benutzerpasswörter müssen Komplexitätsrichtlinien einhalten
- Das Netzwerk wird durch Firewalls und mittels VLAN konfigurierter Netzwerkverteiler abgesichert
- Es werden aktuelle Antivirentechniken eingesetzt, kontrolliert und laufend aktualisiert
- Es werden Stichprobenkontrollen der IT Sicherheitsmaßnahmen durchgeführt

III. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Es gilt das Datensparsamkeitsprinzip (Daten werden, wenn möglich nicht gespeichert)
- DV Anlagen unterliegen einem Zugriffsschutz durch mind. Benutzer/Passwort (siehe *1.II.*)
- Es wird ein Berechtigungsmodell für Daten verwendet basierend auf Funktion und Arbeitsprofil
    - Die Berechtigungsbewilligung (organisatorisch) und die Berechtigungsvergabe (technisch) sind getrennt
- DV Anlage werden bei Nichtbenutzung gesperrt
- Es werden Stichprobenkontrollen der IT Sicherheitsmaßnahmen durchgeführt

IV. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Es erfolgt eine technische Trennung von Produktiv und Testsystemen
- Es erfolgt eine Trennung bei der Verarbeitung personenbezogener Daten nach Tätigkeitsprofil und Abteilungszuordnung
- Es erfolgt eine Trennung bei der Verarbeitung personenbezogener Daten durch ein abgestuftes Berechtigungsmodell nach Abteilung, Position und Tätigkeit

V. Pseudonymisierung

Maßnahmen, die gemäß Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO, gewährleisten, dass verarbeitete Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

- Eine Psedonymisierung erfolgt in Testsystemen, sowie bei temporär vorhandenen Sicherungen von IT-Kommunikationslösungen, bzw. der IT Infrastruktur. Personenbezogene Kundendaten sind hierbei physikalisch getrennt von technischen Daten aus IT-Kommunikationslösungen/IT Infrastruktur und bieten demnach keine Rückschlüsse aufeinander.

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

I. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Es gilt das Datensparsamkeitsprinzip (Daten werden, wenn möglich nicht gespeichert)
- Datenübertragungen erfolgen nur über gesicherte Verbindungen
- Datenträgerschnittstellen sind „nur lesend“ geschaltet
- Mobile DV-Anlagen sind zugriffsgeschützt durch mind. Benutzer/Passwort (siehe *1.II.*)
- Es wird ein Berechtigungsmodell für Daten verwendet (siehe *1.III.*)
- defekte und nicht mehr genutzte Datenträger werden protokolliert vernichtet

II. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Fernwartungsaufgaben und durchgeführte Fernwartungen werden im Ticketsystem und ggf. Serviceobjekt dokumentiert

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

- Es gilt das Datensparsamkeitsprinzip (Kundendaten werden, wenn möglich nicht gespeichert)
- Es erfolgt eine ständig verfügbare Absicherung vor Stromschwankungen via USV Anlagen
- Eine Datensicherung von Daten und Produktivservern sichert wie folgt
    - Sicherung der gesamten VM, täglich, digital auf abgesicherten HDD, Vorhalt: 3 Tage
    - Sicherung von Datenbanken, täglich sowie b.B., digital auf abgesicherten HDD, Vorhalt: 3 Tage
    - Sicherung von Dateien, wöchentlich, digital auf abgesicherten HDD
- Standard Brandschutzmaßnahmen sind im Einsatz
- Der Zugangsschutz zu Datenspeichern ist mind. via Benutzer/Passwort (siehe *1.II.*) gewährleistet
- Der Zutrittsschutz zu Datenspeichern wird via elektronischem Schloss realisiert

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

I. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- Arbeitsanweisung zum Datenschutz werden und wurden erstellt sowie dokumentiert
- Es erfolgt eine Verarbeitung im Auftrag mit standardisierten Vertragsformularen des Auftragsverarbeiters, um eine gleichbleibende Qualität der Auftragsverarbeitung zu gewährleisten. Davon ggf. abweichende Formulare des Auftraggebers werden ggü. den betroffenen Beschäftigten des Auftragsverarbeiters besonders gekennzeichnet, um Abweichungen in den Standards der Arbeitsabläufe zu erfassen

II. Evaluierung

Maßnahmen, zur Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Datenschutz-Management
- Es erfolgt eine Auftragskontrolle (siehe *4.I.*)
- Es erfolgen und erfolgten Einweisungen und Schulungen der Mitarbeiter