Datenschutzvertrag

Vereinbarung über Datenverarbeitung im Auftrag

zwischen Arbeitgeber

Arbeitgebername GmbH

(Verantwortlicher – im Folgenden „Auftraggeber“)

und

Caldera Service GmbH, Borsteler Chaussee 51, 22453 Hamburg

(Auftragsverarbeiter – im Folgenden „Auftragnehmer“)

Hauptinformationen	
Datum dieses Datenschutzvertrags	27.03.2024
Laufzeit dieses Datenschutzvertrags	gem. Dienstleistungsvertrag
ID/Name und Datum des Hauptvertrags	Dienstleistungsvertrag
Name, Kontaktdaten und Benennungsdatum des Datenschutzbeauftragten des Auftragnehmers	Herr Dietmar Niehaus (Best Carrier GmbH, Anne-Conway- Straße 1, 28359 Bremen), 01. Januar 2019
Datenschutzbeauftragter des Auftraggebers	Maßgeblich ist der aktuell benannte und veröffentlichteDatenschutzbeauftragte des Auftraggebers
Liste der Anlagen	**Anlage 1**: Übersicht über Daten und Verarbeitungstätigkeiten **Anlage 2**: Genehmigte Unterauftragnehmer **Anlage 3**: Technische und organisatorische Maßnahmen (Sicherheitskonzept)

1. Allgemein

1.1 Vertragsgegenstand

Dieser Datenschutzvertrag regelt die Pflichten des Auftragnehmers als Auftragsverarbeiter im Zusammenhang mit der Erbringung der vertragsgegenständlichen Leistungen gemäß dem Dienstleistungsvertrag („**Hauptvertrag**“).

Der Auftragnehmer nimmt die in **Anlage 1** zu diesem Datenschutzvertrag im Einzelnen beschriebenen Verarbeitungstätigkeiten vor. Die Verarbeitungszwecke und die Kategorien der zu verarbeitenden personenbezogenen Daten sowie die Kategorien der betroffenen Personen sind ebenfalls in **Anlage 1** zu diesem Datenschutzvertrag beschrieben.

1.2 Auslegung und Verhältnis zum Hauptvertrag

Die Verwendung der Begriffe „schriftlich“ oder „in schriftlicher Form“ in diesem Datenschutzvertrag schließt E-Mails ein.

Die Anlagen sind Bestandteil dieses Datenschutzvertrags. Jede Bezugnahme auf diesen Datenschutzvertrag schließt auch die Anlagen ein. Bei Widersprüchlichkeiten zwischen den Bestimmungen dieses Datenschutzvertrages und Bestimmungen des Hauptvertrags gehen die Bestimmungen dieses Datenschutzvertrages denen des Hauptvertrags vor, soweit sich die Widersprüchlichkeiten auf die Verwendung personenbezogener Daten beziehen.

2. Definitionen

BEGRIFF	DEFINITION
Datenschutzrechtliche Anforderungen	Bezieht sich auf sämtliche geltenden Gesetze und Regelungen in Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) („**DSGVO**“), sektorspezifischen Regelungen und gültigen Leitfäden und Verhaltenskodizes, die von Aufsichtsbehörden herausgegeben wurden.
Betroffene Person	Bezieht sich auf eine identifizierte oder identifizierbare natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Personenbezogene Daten	Bezieht sich auf jegliche Informationen, die sich auf eine betroffene Person beziehen.

BEGRIFF	DEFINITION
Verarbeitung	Bezieht sich auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
Sicherheitsverstoß	Hat die in Ziffer 9.1 festgelegte Bedeutung.
TOM	Hat die in Ziffer 8.1 festgelegte Bedeutung.

3. Weisungen; Einhaltung von datenschutzrechtlichen Anforderungen

3.1 Weisungen

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich gemäß den Bestimmungen dieses Datenschutzvertrags und den speziellen Einzelweisungen des Auftraggebers. Der Auftragnehmer hat eine Person zu benennen, die hinreichende Fachkenntnis in datenschutzrechtlichen Anforderungen besitzt und berechtigt ist, den Auftragnehmer in Bezug auf diesen Datenschutzvertrag zu vertreten und Weisungen des Auftraggebers entgegenzunehmen. Der Auftraggeber bestätigt mündliche Weisungen unverzüglich in schriftlicher Form. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er der Meinung ist, dass eine Weisung des Auftraggebers möglicherweise gegen datenschutzrechtliche Anforderungen verstößt.

Der Auftraggeber gestattet dem Auftragnehmer eine Datenverarbeitung durch seine Mitarbeiter in Privatwohnungen (Heim- oder Telearbeit bzw. Home-Office) unter den nachfolgenden Bedingungen. Der Auftragnehmer bleibt vollumfänglich verantwortlich, den Datenschutz und die Datensicherheit im Home-Office zu gewährleisten. Insbesondere trifft der Auftragnehmer angemessene Maßnahmen, die der besonderen Verarbeitungssituation des Home-Office gerecht werden und gewährleistet, dass das Sicherheitsniveau der vertraglich vereinbarten Maßnahmen insgesamt nicht unterschritten wird.

Der Auftraggeber weist dabei insbesondere auf folgende, zentrale Maßnahmen hin:

Verbindung ausschließlich über ein sogenanntes Virtual Private Network (VPN) bzw. gesicherte Verbindungen, Verschlüsselung der Daten, geeignete häusliche Räumlichkeiten und Arbeitsmittel zur sicheren Aufbewahrung und vertraulichen Behandlung von Unterlagen und Datenträgern mit personenbezogenen Daten.

3.2 Einhaltung von datenschutzrechtlichen Anforderungen

Der Auftragnehmer hat bei der Verarbeitung personenbezogener Daten die datenschutzrechtlichen Anforderungen einzuhalten. Er hat den Auftraggeber in angemessenem Umfang bei der Abwehr von Ansprüchen zu unterstützen, die gegen diesen aufgrund eines angeblichen Verstoßes gegen datenschutzrechtliche Anforderungen erhoben werden. Insbesondere hat der Auftragnehmer im Falle einer Schadenersatzforderung bzw. eines Bußgeldes wegen behaupteter unzulässiger Datenverarbeitung dem Auftraggeber die noch vorhandenen Dokumentationen zur Führung des Entlastungsbeweises auch nach Vertragsende unverzüglich nach Aufforderung durch den Auftraggeber zu überlassen.

4. Bereitstellung von Informationen durch den Auftragnehmer und Unterstützung des Auftraggebers

Der Auftragnehmer hat auf Anfrage des Auftraggebers alle Informationen zur Verfügung zu stellen, die zur Erfüllung datenschutzrechtlicher Anforderungen erforderlich sind. Darüber hinaus hat er den Auftraggeber bei der Einhaltung der datenschutzrechtlichen Anforderungen zu unterstützen. Dies betrifft insbesondere die Unterstützung des Auftraggebers bei der Einhaltung des Grundsatzes von „privacy by design“ (Datenschutz durch Technikgestaltung), der Erstellung von Verzeichnissen von Verarbeitungstätigkeiten, der Zusammenarbeit mit der relevanten Aufsichtsbehörde sowie bei Meldungen an diese, der Sicherheit der Verarbeitung sowie der Durchführung von Datenschutz-Folgenabschätzungen.

5. Weiterer Transfer personenbezogener Daten

Der Auftragnehmer darf personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten bzw. an Empfänger außerhalb des Europäischen Wirtschaftsraum weitergeben, sofern er vertragliche Vereinbarungen schließt, mit denenein angemessenes Datenschutzniveau im Sinne der datenschutzrechtlichen Anforderungen sichergestellt wird und die gemäßden datenschutzrechtlichen Anforderungen vorgeschrieben und/oder von der jeweiligen Aufsichtsbehörde genehmigt wordensind. Diese können insbesondere die EU-Standardvertragsklauseln für den Transfer personenbezogener Daten an Auftragsverarbeiter in Drittländern oder verbindliche interne Datenschutzvorschriften sein.

6. Unterauftragsverhältnisse

6.1 Informationspflicht und Widerspruchsrecht

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu

gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- oder Transportdienstleistungen in Anspruch nimmt. Der Auftragnehmer darf nur die in **Anlage 2** zu diesem Datenschutzvertrag aufgeführten Unterauftragnehmer im Zusammenhang mit den vertragsgegenständlichen Leistungen beauftragen. Die Beauftragung weiterer Unterauftragnehmer oder Änderung bestehender Unterauftragsverhältnisse ist dem Auftraggeber vorher anzuzeigen, wobei dieser die Möglichkeit erhält, hiergegen Einspruch zu erheben.

6.2 Beauftragung von Unterauftragnehmern

Der Auftragnehmer hat alle Unterauftragnehmer sorgfältig auszuwählen. Dies gilt insbesondere im Hinblick auf deren Einhaltung der datenschutzrechtlichen Anforderungen. Der Auftragnehmer hat mit jedem genehmigten Unterauftragnehmer geeignete schriftliche Vertragsvereinbarungen zu schließen, die diesem dieselben Pflichten auferlegen, die in diesem Datenschutzvertrag zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind. Darüber hinaus haben die Vertragsvereinbarungen den Unterauftragnehmer zur Einhaltung der datenschutzrechtlichen Anforderungen zu verpflichten. Dies betrifft insbesondere die Vertraulichkeitspflicht, etwaige Pflichten hinsichtlich beruflicher Qualifikation und Schulung von Mitarbeitern sowie Meldepflichten bei Datenschutzverletzungen. Ferner haben sie dem Auftraggeber dieselben Rechte gegenüber dem Unterauftragnehmer einzuräumen wie dem Auftragnehmer (insbesondere Prüfungs- und Einsichtsrechte), wobei etwaige Prüfungen bei Unterauftragnehmern im Beisein des Auftragnehmers stattzufinden haben.

Der Auftraggeber hat das Recht, Kopien der entsprechenden Vertragsvereinbarungen zwischen dem Auftragnehmer und seinen Unterauftragnehmern zu verlangen. Hierbei ist der Schutz von Betriebs- und Geschäftsgeheimnissen angemessen zu berücksichtigen.

Ziffer 5 gilt sinngemäß, wenn der Auftragnehmer einen Unterauftragnehmer mit der Erbringung einer vertragsgegenständlichen Leistung außerhalb des Europäischen Wirtschaftsraums beauftragen möchte.

7. Vertraulichkeit, Rückgabe und Vernichtung von personenbezogenen Daten

7.1 Vertraulichkeit und Benachrichtigungen

Der Auftragnehmer hat bei der Verarbeitung personenbezogener Daten im Rahmen dieses Datenschutzvertrags das Datengeheimnis sowie Vertraulichkeit zu wahren. Er hat das Gleiche von sämtlichen mit der Erbringung der vertragsgegenständlichen Leistungen betrauten Personen zu verlangen. Der Auftragnehmer hat daher bei der Verarbeitung von personenbezogenen Daten nur solche Personen einzusetzen, die ordnungsgemäß angewiesen und zur Vertraulichkeit

verpflichtet wurden und die angemessen und regelmäßig zu den datenschutzrechtlichen Anforderungen geschult wurden, die für ihre Tätigkeit relevant sind. Auf Nachfrage des Auftraggebers hat der Auftragnehmer die Erfüllung dieser Pflichten nachzuweisen.

Auftraggeber und Auftragnehmer behandeln sämtliche nicht öffentlich bekannten Angelegenheiten und insbesondere die Geschäfts- und Betriebsgeheimnisse des jeweils anderen streng vertraulich und nutzen entsprechende Informationen nur zu den in diesem Datenschutzvertrag aufgeführten Zwecken. Sie verpflichten sich, solche Informationen weder aufzuzeichnen noch weiterzugeben oder zu verwerten. Ferner verpflichten sie sich, auch über das Ende des Vertragsverhältnisses hinaus, zeitlich unbegrenzt Stillschweigen über die ihnen im Zusammenhang mit dem Auftrag bekannt gewordenen Informationen, insbesondere die jeweiligen Datensicherungsmaßnahmen, zu wahren.

7.2 Informationspflichten

Der Auftragnehmer hat den Auftraggeber zu informieren, wenn personenbezogene Daten von folgenden Ereignissen bzw. Maßnahmen betroffen sind und sofern diese Ereignisse direkte Auswirkung auf dieses Auftragsverhältnis hat: Revisionen, Prüfungen, Untersuchungen, Durchsuchungen und Beschlagnahmungen, Pfändungsbeschlüsse, Einziehungsentscheidungen im Insolvenzfall oder Insolvenzverfahren, anhängige oder drohende Vollstreckungsverfahren, Vollstreckungsmaßnahmen, eingeleitete oder drohende Gerichtsverfahren gegen den Auftragnehmer oder einen Unterauftragnehmer oder ähnliche Ereignisse bzw. Maßnahmen Dritter.

7.3 Schutz von Privatgeheimnissen

Sofern es sich beim Auftraggeber um ein Unternehmen der privaten Kranken-, Unfall- oder Lebensversicherung handelt bzw. Daten eines solchen Unternehmens im Auftrag verarbeitet werden sollen, ist der Auftragnehmer zusätzlich verpflichtet, alle zum persönlichen Lebensbereich der Versicherungsnehmer und Leistungsempfänger des Auftraggebers gehörenden Geheimnisse sowie Berufs- und Geschäftsgeheimnisse, die dem besonderen strafrechtlichen Schutz des § 203 Abs. 1 Nr. 7 StGB unterliegen und ihm bei oder gelegentlich der Erbringung der vertragsgegenständlichen Leistungen bekannt werden, insbesondere sämtliche Informationen und Daten, die das Versicherungsverhältnis zum Auftraggeber betreffen, einschließlich des Bestehens des Versicherungsverhältnisses selbst, (nachfolgend: „Privatgeheimnisse“) unbefristet streng geheim zu halten, vor dem Zugriff Dritter zu schützen und sie nicht unbefugt zu offenbaren.

Die Verpflichtung zur Geheimhaltung von Privatgeheimnissen erstreckt sich auch auf die vom Auftragnehmer im Rahmen der Durchführung dieses Vertrags eingesetzten Erfüllungsgehilfen. Er wird diese über eine mögliche Strafbarkeit nach § 203 Abs. 1 Nr.7 i.V.m. § 203 Abs. 4 StGB aufklären, ihnen den Regelungen dieses Paragraphen entsprechende Geheimhaltungspflichten auferlegen und dies dem Auftraggeber auf Verlangen nachweisen. Dies gilt auch, wenn sich der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten weiterer Unterauftragnehmer bedient.

7.4 Löschung oder Rückgabe personenbezogener Daten

Der Auftragnehmer darf personenbezogene Daten nur so lange behalten, wie dies zur Erfüllung der Verarbeitungszwecke gemäß diesem Datenschutzvertrag notwendig ist. Der Auftragnehmer darf ohne vorherige schriftliche Genehmigung des Auftraggebers keine Kopien oder Duplikate der Daten erstellen. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Kündigung oder Ablauf des Hauptvertrags hat der Auftragnehmer auf Anforderung des Auftraggebers sämtliche Dokumente, Verarbeitungs- und Arbeitsergebnisse, digitale Datenträger sowie Datensätze im Zusammenhang mit den vertragsgegenständlichen Leistungen zu löschen bzw. in einem strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber zurückzugeben.

Auch bei Störungen im Betriebsablauf, etwa bei Hardwaretausch, hat der Auftragnehmer dafür Sorge zu tragen, dass keine Daten des Auftraggebers an Dritte weitergegeben bzw. dass Daten auf der auszutauschenden Hardware vor der Weitergabe unwiederbringlich gelöscht werden.

Der Auftragnehmer garantiert dem Auftraggeber die ordnungsgemäße Vernichtung nicht benötigten Datenmaterials (Probeausdrucke, überzählige Listen usw.). Zu entsorgende Unterlagen sind nach DIN 66399-1 der Schutzstufe 2 zuzuordnen und deshalb mit einem Aktenvernichter unleserlich zu machen, der nach DIN 66399 mindestens die Anforderungen der Sicherheitsstufe 4 erfüllt. Sollte eine höhere Stufe erforderlich sein, teilen Auftraggeber und Auftragnehmer sich dies jeweils mit.

Der Auftragnehmer hat schriftlich zu bestätigen, dass er den Anforderungen gemäß dieser Ziffer nachgekommen ist und hat dies auf Anforderung des Auftraggebers durch Vorlage eines Löschprotokolls nachzuweisen.

Der Auftragnehmer hat sämtliche Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung personenbezogener Daten gemäß diesem Datenschutzvertrag dienen, über die Laufzeit des Hauptvertrags hinaus entsprechend der gesetzlichen Aufbewahrungsfristen aufzubewahren.

8. Technische und organisatorische Maßnahmen (Sicherheitskonzept);Verzeichnisse

8.1 Technische und organisatorische Maßnahmen

Der Auftragnehmer hat betriebliche, verwaltungstechnische, physische, technische und organisatorische Maßnahmen („TOM“) zum Schutz der personenbezogenen Daten vor zufälliger, unbefugter oder unrechtmäßiger Zerstörung, Verlust, Veränderung, Weitergabe oder Zugriff zu implementieren, die den datenschutzrechtlichen Anforderungen entsprechen.

Hierbei sind das Risiko für die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gemäß den datenschutzrechtlichen Anforderungen zu berücksichtigen. Die TOM des Auftragnehmers müssen zu jeder Zeit eine strenge Trennung von personenbezogenen Daten, die im Rahmen dieses Datenschutzvertrags verarbeitetet werden, den eigenen Daten des Auftragnehmers und den Daten anderer Kunden des Auftragnehmers sicherstellen. Die vom Auftragnehmer zum Zeitpunkt dieses Datenschutzvertrags implementierten TOM sind in **Anlage 3** zu diesem Datenschutzvertrag (Sicherheitskonzept) aufgeführt.

Der Auftragnehmer sichert zu, dass bei mobilem Arbeiten die Einhaltung der erforderlichen TOM gemäß Sicherheitskonzept sichergestellt ist, wenn personenbezogene Daten im Rahmen dieses Auftragsverhältnisses verarbeitet werden.

8.2 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragnehmer hat gemäß den datenschutzrechtlichen Anforderungen ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

9. Sicherheitsverstöße

9.1 Benachrichtigungspflicht

Der Auftragnehmer hat den Auftraggeber in folgenden Fällen zu benachrichtigen: (i) Wenn er den Verlust von oder den unbefugten Zugriff auf von ihm oder einem Unterauftragnehmer gespeicherte personenbezogene Daten entdeckt oder hiervon Kenntnis erlangt oder (ii) wenn er oder ein Unterauftragnehmer gegen datenschutzrechtliche Anforderungen verstößt („**Sicherheitsverstoß**“). Die Meldung an den Auftraggeber hat unverzüglich, spätestens jedoch innerhalb von 72 Stunden, zu erfolgen und muss so umfassend wie möglich sein. Sie soll insbesondere folgende Angaben enthalten: (i) Art des Sicherheitsverstoßes, (ii) wahrscheinliche Folgen des Sicherheitsverstoßes sowie (iii) ergriffene oder vorgeschlagene Maßnahmen zur Behebung des Sicherheitsverstoßes. Zusätzlich hat der Auftragnehmer dem Auftraggeber im Fall eines Sicherheitsverstoßes künftig durchzuführende Maßnahmen zur Verhinderung gleicher oder ähnlicher Sicherheitsverstöße zu melden.

9.2 Benachrichtigung von Einzelpersonen bei Sicherheitsverstößen und Abhilfemaßnahmen

Soweit der Auftraggeber eine betroffene Person im Fall eines Verlusts ihrer personenbezogenen Daten oder eines unbefugten Zugriffs hierauf gemäß den datenschutzrechtlichen Anforderungen benachrichtigen muss, hat der Auftragnehmer diesen hierbei in angemessenem Umfang zu unterstützen.

10. Berichtigung, Einschränkung und Löschung; Rechte von betroffenen Personen

Der Auftragnehmer darf ohne schriftliche Weisung des Auftraggebers personenbezogene Daten nicht berichtigen oder löschen bzw. ihre Verarbeitung einschränken. Sollte sich eine betroffene Person direkt an den Auftragnehmer wenden und Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder Übertragung ihrer personenbezogenen Daten verlangen, hat der Auftragnehmer diese Anfrage unverzüglich an den Auftraggeber weiterzuleiten.

Der Auftragnehmer hat TOM zu implementieren, die es dem Auftraggeber ermöglichen, die entsprechenden datenschutzrechtlichen Anforderungen einzuhalten. Er hat auch sonst den Auftraggeber in angemessenem Umfang dabei zu unterstützen, auf Anfragen von betroffenen Personen zu reagieren, die ihre Rechte im Zusammenhang mit ihren personenbezogenen Daten ausüben. Er hat den Auftraggeber auf dessen Anfrage insbesondere durch folgende Maßnahmen zu unterstützen: (i) Er hat dem Auftraggeber eine Kopie der personenbezogenen Daten der betroffenen Person in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung zu stellen oder (ii) nach Wahl des Auftraggebers angemessenen Zugriff auf die personenbezogenen Daten zu gewähren und (iii) dem Auftraggeber alle Informationen zur Datenverarbeitung zur Verfügung zu stellen.

11. Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer muss ein Datenschutzbeauftragter benannt sein.

Der Datenschutzbeauftragte hat die Einhaltung der datenschutzrechtlichen Anforderungen im Hinblick auf das Auftragsverhältnis auf Auftragnehmerseite, auch hinsichtlich der Unterauftragnehmer, zu überwachen.

12. Prüfungen

Der Auftragnehmer gestattet dem Auftraggeber, den vom Auftraggeber ernannten Prüfern und den zuständigen Aufsichtsbehörden seine Verarbeitungsprozesse (einschließlich der Umsetzung von TOM) zu prüfen. Die genannten Stellen dürfen auch prüfen, ob der Auftragnehmer die Weisungen des Auftraggebers befolgt und die datenschutzrechtlichen Anforderungen einhält. Der Auftragnehmer hat diesen Stellen bzw. ihren vertretungsberechtigten Personen alle hierfür notwendigen Informationen zur Verfügung zu stellen und ihnen etwaige erforderliche Zutritts- und Zugriffsrechte einzuräumen (z.B. Zutrittsrecht zum Betriebsgelände und Zugriffsrecht auf die Datenbestände). Der Auftragnehmer hat das Gleiche bei seinen Unterauftragnehmern sicherzustellen.

Der Auftragnehmer hat regelmäßig zu überprüfen, ob er und seine Unterauftragnehmer diesen Datenschutzvertrag, den Hauptvertrag und die datenschutzrechtlichen Anforderungen im Zusammenhang mit der Datenverarbeitung einhalten. Sollte sich bei einer solchen Prüfung herausstellen, dass der Auftragnehmer bzw. dessen Verarbeitung personenbezogener Daten von den datenschutzrechtlichen Anforderungen oder den Bestimmungen dieses Datenschutzvertrages und / oder des Hauptvertrages abweicht, ist der Auftraggeber schriftlich hiervon zu informieren.

Sofern Prüfungen der Aufsichtsbehörden beim Auftraggeber stattfinden, die ganz oder teilweise diesen Datenschutzvertrag betreffen, verpflichtet sich der Auftragnehmer, den Auftraggeber im Rahmen dieses Datenschutzvertrags zu unterstützen sowie die entsprechende Unterstützung durch seine Unterauftragnehmer sicherzustellen.

Sofern eine Aufsichtsbehörde, die für den Auftraggeber zuständig ist, eine Prüfung beim Auftragnehmer oder dessen Unterauftragnehmer durchführt, hat diese Prüfung im Beisein des Auftraggebers stattzufinden.

Sofern Prüfungen beim Auftragnehmer durch die für diesen zuständigen Aufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer, den Auftraggeber darüber zu informieren und ihm insbesondere Feststellungen mit unmittelbarer oder mittelbarer Auswirkung für das Auftragsverhältnis bekanntzugeben.

13. Zugriff auf DV-Ressourcen / Dialogsysteme des Auftraggebers

Soweit der Auftragnehmer bzw. von ihm beauftragte Personen im Zusammenhang mit der Vertragserfüllung Zugriff auf DV-Ressourcen des Auftraggebers (Dialogsysteme, Datenbanken usw.) haben, ist mit diesen Ressourcen sorgfältig und bestimmungsgemäß umzugehen; sie dürfen weder zerstört, verfälscht noch auftragswidrig eingesetzt werden.

Zusätzlich gelten bei der Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, folgende Bestimmungen:

a. Der Auftragnehmer hat gemeinsam mit dem Auftraggeber Verfahrenszweck, betroffene Datenarten, Zugriffsberechtigte sowie erforderliche besondere Sicherheitsvorkehrungen festzulegen.
b. Der Auftragnehmer trägt die Verantwortung für die Zulässigkeit jedes einzelnen Abrufs.
c. Der Auftragnehmer hat gemeinsam mit dem Auftraggeber zu gewährleisten, dass die Zulässigkeit jedes Abrufs kontrolliert werden kann.
d. Der Auftragnehmer hat dem Auftraggeber zu diesem Zweck Stichprobenprüfungen gemäß gesonderter Vereinbarung zu gestatten und die Führung der erforderlichen Einzelnachweise zu gewährleisten.

14. Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seine Pflichten aus diesem Datenschutzvertrag nicht nachkommt oder Sicherheitsregeln vorsätzlich oder grob fahrlässig verletzt. Insbesondere das Einleiten eines Vergleichs- oder Insolvenzverfahrens stellt einen wichtigen Grund zur Kündigung des Hauptvertrags dar.

Der Auftraggeber ist berechtigt, bereits bei einem einmaligen Verstoß gegen die Sicherheitsvorschriften den Austausch der betreffenden Personen zu verlangen bzw. das Vertragsverhältnis mit sofortiger Wirkung zu beenden. Weitergehende Rechte des Auftragnehmers bleiben hiervon unberührt.

15. Laufzeit dieses Datenschutzvertrags

Die Laufzeit dieses Datenschutzvertrags entspricht der Laufzeit des Hauptvertrags. Der Ablauf oder die Kündigung des Hauptvertrags entbindet die Parteien nicht von ihren jeweiligen Pflichten hinsichtlich der Datensicherheit und des Schutzes personenbezogener Daten, solange wie eine Verarbeitung dieser Daten nach Ablauf oder Kündigung noch erfolgt.

Sollte eine oder mehrere der vorstehenden Bestimmungen ganz oder teilweise unwirksam oder lückenhaft sein oder werden, wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Der Auftraggeber und der Auftragnehmer verpflichten sich, die unwirksame oder lückenhafte Bestimmung durch eine solche wirksame zu ersetzen, die dem wirtschaftlichen Zweck und dem Willen der Vertragsparteien am nächsten kommt.

ANLAGE 1: Übersicht über Daten und Verarbeitungstätigkeiten

1. Beschreibung des Zwecks und der Art der Verarbeitung personenbezogener Daten:

Auf FirmenOnline kann sich der Arbeitgeber für bAV-Verträge, die er für seine Mitarbeiter bei der Allianz Lebensversicherungs-AG, der Allianz Pensionskasse AG oder der Allianz Pensionsfonds AG (im Folgenden: „Allianz-Verträge“) abgeschlossen hat, kostenfrei die Versicherungsdaten anzeigen lassen und zu den betreffenden Verträgen Services der Allianz auslösen. Auch bAV-Verträge, die der Arbeitgeber bei anderen Versorgungseinrichtungen (Versicherungsunternehmen, Unterstützungskassen, Versorgungswerken usw.; im Folgenden zusammen: „Versicherer“) für seine Mitarbeiter unterhält (im Folgenden: „Verträge weiterer Versicherer“), kann sich der Arbeitgeber auf FirmenOnline anzeigen lassen, sofern er deren Versicherungsnummer, Versicherungsnehmer, Versicherer sowie versicherte Person einschließlich Name, Vorname, Geburtsdatum, Beitrag, Förderart und Versicherungsbeginn (im Folgenden zusammen: „Basisdaten“) per Excel-Upload eigenständig und kostenfrei in FirmenOnline hochgeladen hat (im Folgenden: „Vertragsimport“).

Die bAV-Verträge werden hierbei in sog. Vertragsgruppen gebündelt, wobei die Allianz-Verträge und die Verträge weiterer Versicherer jeweils separate Vertragsgruppen bilden. Für Verträge weiterer Versicherer die sogenannten Vertragsgruppen, für Allianz Verträge gemäß der Allianz Gruppenvertragsnummer. Hierfür arbeitet die Allianz mit dem Auftragnehmer zusammen.

Der Auftragnehmer ist ein unabhängiges Fachunternehmen, das Arbeitgeber mit Serviceleistungen im Bereich der Verwaltung von Verträgen der bAV und der Berufsunfähigkeitsabsicherung ihrer Mitarbeiter unterstützt.

Zukünftig soll der Auftraggeber die Möglichkeit haben, auch für seine auf FirmenOnline hochgeladenen Verträge weiterer Versicherer entsprechende Services zu deren Verwaltung zu aktivieren. Hierfür arbeitet die Allianz mit dem Auftragnehmer zusammen. Zum einen soll der Arbeitgeber kostenpflichtig Änderungsaufträge zu den Basisdaten seiner Verträge weiterer Versicherer erteilen können, die vom Auftragnehmer an den Versicherer weitergeleitet und nachgehalten werden.

Zum anderen soll der Auftraggeber den Auftragnehmer kostenpflichtig damit beauftragen können, noch nicht erfasste Daten und Informationen zu seinen Verträgen weiterer Versicherer (wie z.B. zu garantierten Leistungen, Tarifen, Beitragszahlungen oder Vertragsstatus) beim Versicherer anzufragen, um die Basisdaten um diese Datensätze und Informationen anzureichern und diese auf FirmenOnline anzuzeigen. Die Erbringung dieser Services erfolgt hierbei auf Basis des Hauptvertrags.

Für den Abschluss dieses Hauptvertrags und die Beauftragung der Services hält der Auftragnehmer ein Buchungsportal, das ausschließlich über FirmenOnline erreicht werden kann, sowie einen Vertrags- und Datenservice bereit, der über das Buchungsportal kostenpflichtig hinzugebucht werden kann. Des Weiteren unterhält der Auftragnehmer eine Schnittstelle zu FirmenOnline, über die er FirmenOnline so an seine Systeme und Datenbanken anbindet, dass er einerseits zur Ausführung der Serviceaufträge des Auftraggebers die von diesem in FirmenOnline hochgeladenen Basisdaten zu den jeweiligen Verträgen weiterer Versicherer abrufen kann, andererseits die vom Auftragnehmer entsprechend angereicherten und geänderten Datensätze zu den Verträgen weiterer Versicherer wiederum nach FirmenOnline gespiegelt und dort angezeigt werden können.

Hierzu erteilt der Auftraggeber in seiner Funktion als Versicherungsnehmer bzw. Trägerunternehmen dem Auftragnehmer mit Schließung des Hauptvertrags die Vollmacht, in seinem Namen Aufträge zu übermitteln und Korrespondenzen mit den betreffenden Versorgungseinrichtungen zu führen. Als Versicherungsnehmer bzw. Trägerunternehmen erteilt der Auftraggeber der Versorgungseinrichtung mit der Unterzeichnung des „Dienstleistungsvertrages betriebliche Altersversorgung zwischen Auftraggeber und Auftragnehmer“ die Weisung, jeglichen Schriftwechsel, der im Zusammenhang mit erteilten Aufträgen an den Auftragnehmer zu führen ist, elektronisch, telefonisch oder postalisch mit dem Auftragnehmer zu führen. Dies gilt ausdrücklich auch für die Zusendung von Schriftstücken. Schriftstücke des jeweiligen Versicherers werden vom Auftragnehmer digitalisiert. Die digitalisierten Schriftstücke erhält der Auftraggeber zur Abholung per Downloadlink. Der Downloadlink wird bei jedem Posteingang von Schriftstücken an eine im Buchungsprozess anzugebende Mailadresse des Auftraggebers geschickt. Die Authentifizierung des Auftraggebers erfolgt im Rahmen des Buchungsprozesses mit einem Zwei-Faktor Verfahren.

2. Verarbeitungstätigkeiten

- Erhebung
- Strukturierung
- Speicherung
- Einsichtnahme
- Weitergabe
- Abgleich
- Abstimmung oder Kombination
- Löschung
- Sonstige Arten, personenbezogene Daten verfügbar zu machen (z. B. Kommunikation, Nutzung)
- Aufzeichnung
- Modifizierung, Anpassung oder Änderung
- Extraktion
- Offenlegung durch Übertragung
- Vernetzung
- Beschränkung

- Vernichtung
- Abruf

3. Kategorien betroffener Personen

- Mitarbeiter
- Versicherungs- / Vertragsnehmer
- Versicherte Personen
- Vermittler (Vertreter / Makler…)

4. Kategorien personenbezogener Daten

- Rassische oder ethnische Herkunft
- Philosophische Überzeugungen
- Biometrische Daten
- Sexuelle Orientierung
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Gesundheitsdaten
- Strafrechtliche Verurteilungen und Straftaten
- Religion/ Glaube
- Genetische Daten

Keine der genannten Ausprägungen wird gespeichert.

Weitere personenbezogene Daten

Kommunikationsdaten (z.B. Adressen, Telefon, E-Mail) Vertragsabrechnungs- und Zahlungsdaten

ANLAGE 2: Genehmigte Unterauftragnehmer

Unterauftragnehmer 1	
Firmenname des Unterauftragnehmers	akquinet data center competence GmbH
Sitz des Unterauftragnehmers	Ulzburger Straße 201 22850 Norderstedt
Betriebsgelände des Unterauftragnehmers, wo die Datenverarbeitung stattfindet	Paul-Stritter-Weg 5 22297 Hamburg
Zweck der Verarbeitung der Daten des Verantwortlichen durch den Unterauftragnehmer	Betrieb des TÜV-IT zertifizierten Rechenzentrums
Verarbeitungstätigkeiten	Keine
Kategorien betroffener Personen	Keine
Kategorien personenbezogener Daten	Keine
Besondere Kategorien personenbezogener Daten	Keine
Kontaktdaten des Ansprechpartners für Datenschutzfragen beim Unterauftragnehmer (z. B. Datenschutzbeauftragter)	Datenschutzbeauftragter Herr Janos Frank Elisabeth Flügge Straße 8a 22337 Hamburg

Die folgenden Unternehmen werden hiermit im Voraus berechtigt, als Unterauftragnehmer des Auftragnehmers Verarbeitungstätigkeiten auszuführen:

Unterauftragnehmer 2	
Firmenname des Unterauftragnehmers	IT Warehouse AG
Sitz des Unterauftragnehmers	Borsteler Chaussee 51, 22453 Hamburg
Betriebsgelände des Unterauftragnehmers, wo die Datenverarbeitung stattfindet	Borsteler Chaussee 51, 22453 Hamburg
Zweck der Verarbeitung der Daten des Verantwortlichen durch den Unterauftragnehmer	Betrieb und Entwicklung der Verwaltungssoftware
Verarbeitungstätigkeiten	Analog Caldera Service GmbH im Rahmen von BPO
Kategorien betroffener Personen	Analog Caldera Service GmbH im Rahmen von BPO
Kategorien personenbezogener Daten	Analog Caldera Service GmbH im Rahmen von BPO
Besondere Kategorien personenbezogener Daten	Analog Caldera Service GmbH im Rahmen von BPO

Unterauftragnehmer 2	
Kontaktdaten des Ansprechpartners für Datenschutzfragen beim Unterauftragnehmer (z. B. Datenschutzbeauftragter)	Herr Dietmar Niehaus (Best Carrier GmbH, Anne-Conway-Straße 1, 28359 Bremen)

ANLAGE 3: Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen (Art. 32 DS-GVO), um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Diese Maßnahmen schließen Folgendes ein:

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

Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehren:

Die Zutrittskontrolle zu den Räumen des Auftragsnehmers erfolgt durch ein Schließsystem. Die Räume sind permanent verschlossen. Externe werden während der gesamten Aufenthaltsdauer von einem Mitarbeiter des Auftragnehmers begleitet.

Die Serverräume befinden sich in einem externen Hochverfügbarkeits- und Hochsicherheits-Rechenzentrum. Außerhalb der Arbeitszeiten sind die Räume des Auftragnehmers durch eine Einbruchmeldeanlage inkl. Kameraüberwachung gesichert.

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Es bestehen Vorgaben zum Aufbau der Passwörter (Länge von mindestens acht Zeichen; inhaltliche Komplexität: systemseitige Prüfung, Kombination von Groß- und Kleinschreibung, Zahlen und ggf. Sonderzeichen; systemseitige Prüfung der Passwortvorgaben).

Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen

Weitere Maßnahmen: Die Zugangskontrolle erfolgt durch eine kennwortgeschützte Benutzeranmeldung am System.

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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Verpflichtend: Regelungen zur Entsorgung von Papierdokumenten (Schreddergerät oder durch einen zertifizierten Dienstleister mit Entsorgungsbescheinigung). Datenträgervernichtung nach der DIN 66399 mit mindestens Schutzklasse 3.

Weitere Maßnahmen: Die Zugriffskontrolle zu dem System mit den Kundendaten des Auftragnehmers erfolgt durch ein dezidiertes Berechtigungskonzept.

Trennungskontrolle

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

Das Trennungsgebot wird über ein Berechtigungssystem realisiert. Von anderen Anwendungen kann nicht auf die Kundendaten des Auftraggebers zugegriffen werden. Der Auftragnehmer verarbeitet oder nutzt die personenbezogenen Daten des Auftraggebers ausschließlich im Rahmen der vertraglichen Vereinbarungen und der speziellen Einzelanweisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke.

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

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

Eine Pseudonymisierung der Daten durch den Auftragnehmer ist nach dem Auftragszweck aktuell nicht vorgesehen,technisch grundsätzlich jedoch möglich. Dabei kann der Auftraggeber bestimmen, in welchem Maße die Daten pseudonymisiert werden sollen.

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

Weitergabekontrolle

Maßnahmen, die 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:

Verpflichtend ist, bei der Übermittlung personenbezogener Daten mindestens eine der folgenden technischen Vorgaben zu erfüllen:

Verschlüsselungsstandard: Standard Perfect Forward Secrecy, Mindestens TLS Version 1.2 und Schlüssellänge von mindestens 128 Bit (insbesondere keine Verschlüsselung, die auf dem Stromchiffre-Algorithmus RC4 beruht oder auf einfachen DES-Algorithmen und auch keine HDx-Hash-Verfahren [z.B. MD2, MD4, HD5]

Weitere Maßnahmen:
Die Weitergabekontrolle erfolgt grundsätzlich durch eine Verschlüsselung der Daten nach dem Standard AES 256 oder höherwertiger.

Eingabekontrolle

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

Die Eingabekontrolle erfolgt anhand des Zugangs und der Berechtigung des Nutzers. Es wird erkannt und protokolliert, wer, wann, welche Änderung vorgenommen hat.

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

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

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

Tägliches Backup, getrennte Aufbewahrung der Sicherungsmedien, Servervirtualisierung, unterbrechungsfreie Stromversorgung (USV), Firewall, Virenschutz

4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Datenschutz-Management (Art. 32 Abs. 1 lit. d DS-GVO)

Regelmäßige (mind. jährliche) Auditierung der Datenschutz- und Datensicherheitsmaßnahmen durch externen Datenschutzbeauftragten.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur den Weisungen des Auftraggebers entsprechend verarbeitet werden:

Der Auftraggeber hat das jederzeitige Recht, eine Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durchführen zu lassen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung personenbezogener Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen.