Datenschutzvertrag

Vereinbarung über Datenverarbeitung im Auftrag

zwischen

_____

(Verantwortlicher – im Folgenden „Auftraggeber“)

und

Allianz Lebensversicherungs-AG
Reinsburgstr. 19
70178 Stuttgart

(Auftragsverarbeiter – im Folgenden „Auftragnehmer“)

Hauptinformationen:

Datum dieses Datenschutzvertrags:	
Laufzeit dieses Datenschutzvertrags:	gekoppelt an die Laufzeit des nachfolgend genannten Hauptvertrags (trägt die Bezeichnung Dienstleistungsvertrag)
ID/Name und Datum des Hauptvertrags:	Gemäß den aktuellen Nutzungsbedingungen von FirmenOnline
Name und Kontaktdaten des Datenschutzbeauftragten des Auftraggebers:	
Name, Kontaktdaten und Benennungsdatum des Datenschutzbeauftragten des Auftragnehmers:	Allianz SE Dirk Weske 80790 München Postfach 11 30, 85774 Unterföhring E-Mail: datenschutz@allianz.de
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 den Nutzungsbedingungen („**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 Datenschutzvertrags und Bestimmungen des Hauptvertrags gehen die Bestimmungen dieses Datenschutzvertrags 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.
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 8.1 festgelegte Bedeutung.
TOM	Hat die in Ziffer 7.1 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.

3.2 Die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen von mobilem Arbeiten (z. B. Telearbeit) ist gestattet, da der Auftragnehmer gewährleistet, dass dafür ausschließlich sichere VPN-Verbindungen in sein Netzwerk genutzt werden und dass eine Kenntnisnahme der Daten durch Dritte ausgeschlossen ist.

3.3 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. Unterauftragsverhältnisse

5.1 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.

5.2 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.

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

6. Vertraulichkeit, Rückgabe und Vernichtung von personenbezogenen Daten

6.1 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.

6.2 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.

6.3 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.

6.4 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 sich dies Auftraggeber und Auftragnehmer 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.

7. Technische und organisatorische Maßnahmen (Sicherheitskonzept); Verzeichnisse

7.1 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 verarbeitet 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.

7.2 Verzeichnis von Verarbeitungstätigkeiten

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

8. Sicherheitsverstöße

8.1 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.

8.2 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.

9. 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 angemessenen 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.

10. Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer muss ein Datenschutzbeauftragter benannt sein. Der Auftragnehmer muss dem Auftraggeber den Datenschutzbeauftragten sowie dessen Ernennungsdatum mitteilen (siehe Deckblatt – Hauptinformationen).

Der Datenschutzbeauftragte hat die Einhaltung der datenschutzrechtlichen Anforderungen im Hinblick auf das Auftragsverhältnis auf Auftragnehmerseite, auch hinsichtlich der Unterauftragnehmer, zu überwachen. Der Auftragnehmer hat dem Auftraggeber einen Wechsel seines Datenschutzbeauftragten unverzüglich anzuzeigen.

11. 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 Datenschutzvertrags und/oder des Hauptvertrags 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 diese 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.

12. 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.

13. 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.

14. 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.

Für den Auftraggeber

Ort, Datum	Unterschrift	Name in Druckbuchstaben
Ort, Datum	Unterschrift	Name in Druckbuchstaben

Für den Auftraggeber

Ort, Datum	Unterschrift	Name in Druckbuchstaben
Ort, Datum	Unterschrift	Name in Druckbuchstaben

ANLAGE 1:
Übersicht über Daten und Verarbeitungstätigkeiten

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

Für die Verwaltung der betrieblichen Altersversorgung bietet die Allianz Lebensversicherungs-AG für Arbeitgeber die digitale Verwaltungsplattform FirmenOnline an. In FirmenOnline sollen neben den Verträgen, die bei der Allianz Lebensversicherungs-AG, der Allianz Pensionskasse-AG oder der Allianz Pensionsfonds-AG abgeschlossen wurden, auch Verträge von anderen Versicherungsunternehmen des Auftraggebers angezeigt werden („FirmenOnline+“). Der Auftraggeber lädt die Daten per Excel Upload selbstständig in das Portal FirmenOnline hoch. Die Daten werden dort zur Anzeige gebracht, aber inhaltlich nicht verarbeitet.

2. Verarbeitungstätigkeiten

- ☒ Erhebung
- ☒ Speicherung
- ☒ Einsichtnahme
- ☒ Weitergabe
- ☒ Abgleich
- ☒ Löschung
- ☒ Sonstige Arten, personenbezogene Daten verfügbar zu machen (z. B. Kommunikation, Nutzung)
- ☒ Aufzeichnung
- ☒ Modifizierung, Anpassung oder Änderung
- ☒ Extraktion
- ☒ Vernichtung
- ☒ Abruf

3. Kategorien betroffener Personen

- ☒ Mitarbeiter
- ☒ Versicherte Personen
- ☒ Vermittler (Vertreter/ Makler…)
- ☒ Sonstige (bitte angeben):
  Dritte, die der Auftragnehmer zugriffsberechtigt

4. Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten		
☒ Keine		

Weitere personenbezogene Daten

Mitarbeiter:

- Name, Vorname
- Kontaktdaten (wie Adresse, Telefonnummer, E-Mail-Adresse)
- Geburtsdatum
- Personalnummer
- Daten zum Arbeitsverhältnis (wie Diensteintritt-/Dienstaustrittsdatum)
- Vertragsnummern
- Angaben zu bei anderen Versicherern/Versorgungsträgern bestehenden betrieblichen Altersversorgungsverträgen

Dritte, die der Auftragnehmer zugriffsberechtigt:

- Name, Vorname
- Kontaktdaten (wie Adresse, Telefonnummer, E-Mail-Adresse)

ANLAGE 2:
Genehmigte Unterauftragnehmer

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

Firmenname des Unterauftragnehmers
Allianz Technology SE (sowie deren Subunternehmer)
Sitz des Unterauftragnehmers
Fritz-Schäffer-Straße 9, 81737 München
Verarbeitungstätigkeiten
Shared-Services-Dienstleistungen für Gesellschaften der Allianz Gruppe
Kontaktdaten des Ansprechpartners für Datenschutzfragen beim Unterauftragnehmer (z. B. Datenschutzbeauftragter)
Knut Weisser E-Mail: knut.weisser@allianz.com

Firmenname des Unterauftragnehmers
IBM Deutschland GmbH
Sitz des Unterauftragnehmers
IBM-Allee 1 71139 Ehningen Postanschrift: 71137 Ehningen
Verarbeitungstätigkeiten
IT-Wartung
Kontaktdaten des Ansprechpartners für Datenschutzfragen beim Unterauftragnehmer (z. B. Datenschutzbeauftragter)
Dr. Stefan Krätschmer E-Mail: skraetsc@de.ibm.com

Firmenname des Unterauftragnehmers
VLS Versicherungslogistik GmbH
Sitz des Unterauftragnehmers
Merlitzstraße 8, 12489 Berlin
Verarbeitungstätigkeiten
Posteingangsbearbeitung
Kontaktdaten des Ansprechpartners für Datenschutzfragen beim Unterauftragnehmer (z. B. Datenschutzbeauftragter)
Dirk Weske Datenschutzbeauftragter für VLS Versicherungslogistik GmbH Postfach 11 30, 85774 Unterföhring E-Mail: datenschutz@allianz.de

ANLAGE 3:
Technische und organisatorische Maßnahmen (Sicherheitskonzept)[1]

1. Einleitung

Die im Folgenden aufgeführten technischen und organisatorischen Maßnahmen (TOM) gelten für die Verarbeitung personenbezogener Daten bei den AZiD Gesellschaften und ihren Tochtergesellschaften.

Jeder Mitarbeitende der AZiD Gesellschaften verpflichtet sich im Rahmen seiner Neueinstellung auf Datenschutz und Geheimhaltung und erhält Kenntnis von den für ihn relevanten Regelungen. Aufgrund der Zugehörigkeit zum Allianz Konzern findet ein Information Security Framework (Verwaltungsregel für Informationssicherheit) bei den AZiD Gesellschaften Anwendung, in dem die Mindestvorgaben für den Schutz von Informationen verbindlich definiert sind.

Es werden technische und organisatorische Maßnahmen nach Artikel 32 DSGVO getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des Letzteren sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung von Daten verbunden sind.

Die Maßnahmen berücksichtigen gemäß Artikel 32 DSGVO folgende Bereiche:

- Pseudonymisierung und Verschlüsselung der Daten
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Sicherstellung der Datenverarbeitung
- Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen
- Verfahren zur kontinuierlichen Überprüfung, Bewertung und Evaluierung der Maßnahmen zur Gewährleistung der sicheren Datenverarbeitung

2. Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten

Im Folgenden werden technische und organisatorische Sicherheitsmaßnahmen beschrieben, die systemübergreifend dem Schutz personenbezogener Daten gemäß den Anforderungen von Artikel 32 DSGVO dienen.

2.1 Vertraulichkeit gemäß Artikel 32 Abs. 1 lit. DSGVO

2.1.1 Zutrittskontrolle

Der Zutritt zu den Liegenschaften der AZiD Gesellschaften wird Unberechtigten verwehrt.

Jeder offizielle Eingang in Liegenschaften der AZiD Gesellschaften verfügt über einen mit Personal ausgestatten Empfang.

Der legitimierte Zutritt in die Liegenschaften der AZiD Gesellschaften erfolgt in der Regel durch das von der Allianz ONE Protective Security Management implementierte elektronische Zutrittskontrollsystem.

Mitarbeitende und Fremdfirmenbeschäftigte erhalten mit Beginn ihrer Tätigkeit für die AZiD Gesellschaften ein Zutrittsmedium (z. B. Ausweis), welches den Zutritt entsprechend ihres hinterlegten Profils legitimiert ermöglicht. Entsprechend der Zutrittserfordernisse können die Profile angepasst werden.

[1] Version 4.1 von Juli 2024

Besucher und Lieferanten (inkl. Handwerker und Dienstleister etc.) legitimieren sich am vorgegebenen Empfang und erhalten entsprechend ihres Zutrittsanliegens einen zeitlich befristeten Besucherausweis.

Die Ausgabe sämtlicher Ausweise und Zutritte wird protokolliert.

Alle Personengruppen müssen sich mittels ihres Zutrittsmediums auf Aufforderung ausweisen können und den Ausweis sichtbar tragen.

Nur legitimierte Personen erhalten Zutritt zu besonderen Sicherheitsbereichen (z. B. Datenverarbeitungsanlagen), die mittels einem mechanischen oder elektronischen Schließsystem abgesichert sind.

Zur Einhaltung der Sicherheitsanforderungen ist Videotechnik im Einsatz.

2.1.2 Zugangskontrolle

Nur legitimierte Personen haben Zugang zu Datenverarbeitungssystemen.

Erforderliche Zugangsrechte werden nur nach entsprechender Legitimation durch Vorgesetzte oder Informationseigentümer gewährt und laufend kontrolliert.

Authentifizierungen erfolgen üblicherweise mittels 2-Faktor Methodik unter Beachtung definierter Passwortregeln und Mechanismen, um vor unautorisiertem Zugriff zu schützen (z. B. Mindestlänge 10 Zeichen, Ablauf nach 90 Tagen, Sperrung nach definierter Anzahl von Fehlversuchen etc.). Single-Sign-On (SSO) ist wo immer möglich im Einsatz.

Zugriffe erfolgen ausschließlich über eine gesicherte VPN-Verbindung.

Verschlüsselungsverfahren sind verpflichtend und abhängig von der Vertraulichkeitseinstufung in der Verwaltungsrichtlinie für Informationssicherheit geregelt und in Anwendung.

USB-Ports und andere externe Schnittstellen sind per Default deaktiviert.

Eine automatische Bildschirmsperre wird bei Inaktivität (15 Minuten) ausgelöst.

Malware-Schutz in unterschiedlichen Formen ist in alle relevanten IT-Systeme implementiert, u. a.: Antivirus-Software, Einschränkungen hinsichtlich der Installation von Software durch Benutzer, rasche Behebung von bekannten System- und Softwareschwachstellen.

2.1.3 Zugriffskontrolle

Zugriffsrechte für Anwendungen und Prozesse werden in der Regel zentral verwaltet.

Dies erfolgt für alle Anwendungen und Prozesse über einheitlich vorgegebene Berechtigungskonzepte und Vergabeprozesse.

Entsprechende Zugriffsberechtigungen werden nach dem „need to know“ Grundsatz unter Wahrung des Vieraugenprinzips bei einem Legitimationsbeauftragten beantragt und durch diesen und/oder den Informationseigentümer legitimiert.

Die Zugriffsberechtigungen werden je nach Vertraulichkeitseinstufung mindestens einmal jährlich auf Notwendigkeit überprüft, um eine effektive Kontrolle der Zugriffsrechte von Benutzern sicherzustellen.

Mindestens privilegierte Zugriffe auf Anwendungen und/oder geschäftskritische Prozesse werden protokolliert.

Alle Anwendungen und Prozesse durchlaufen Risikobewertungen und Informationsklassifizierungen anhand definierter Bewertungsraster. Anhand der Bewertung und Klassifizierung werden kryptographische Lösungen eingesetzt, um vor unautorisierten Zugriffen zu schützen. Dies umfasst u. a. mobile Endgeräte, Datenträger, Kommunikation (E-Mail) etc.

Alle mobilen Endgeräte wie Laptops, Tablets, Smartphones sind verschlüsselt und ein Mobile Device Management System ist im Einsatz.

2.1.4 Trennungskontrolle

Personenbezogene Daten, die unterschiedlichen Zwecken dienen, werden bei den AZiD Gesellschaften physisch bzw. logisch getrennt geführt und verarbeitet.

Entwicklungs- und Produktionsumgebungen sind physisch bzw. logisch getrennt. Auf Entwicklungs- und Testumgebungen wird zudem nur mit Testdaten gearbeitet. Die eingesetzten Systeme bei den AZiD Gesellschaften sind mehrmandantenfähig.

Zugriffsrechte werden aufgabenbezogen, zentral und auf Basis eines Berechtigungskonzepts granular vergeben, so dass nur die für mit der Bearbeitung legitimierten Personen Zugriff auf die Daten besitzen.

2.1.5 Pseudonymisierung (Art. 32 Abs. 1. lit a DSGVO; Art. 25 Abs. 1 DSGVO)

Wenn möglich und sinnvoll, werden Daten pseudonymisiert verarbeitet.

Informationen, die zur Entschlüsselung pseudonymisierter Daten erforderlich sind, werden in getrennten Systemen vorgehalten und wenn nötig verschlüsselt gespeichert. Es werden Verschlüsselungsmethoden nach dem Stand der Technik eingesetzt.

Wie für alle Zugriffs- und Zugangsrechte gilt auch in diesem Bereich, dass nur legitimierte Nutzer auf Daten zugreifen können, die zur Entschlüsselung nötig sind.

Legitimationen werden auf Basis eines Berechtigungskonzepts vergeben.

2.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.2.1 Weitergabekontrolle

Daten werden in den AZiD Gesellschaften nach unterschiedlichen Vertraulichkeitsstufen klassifiziert. Abhängig vom Grad der Vertraulichkeitsstufe ist vorgeschrieben, wie Daten verschlüsselt gespeichert und übertragen werden müssen.

E-Mails werden verschlüsselt (TLS, S/MIME) übertragen und autorisierte Zugriffe werden technisch über VPN-Technologien und/oder zertifikatsbasierte Authentifizierung legitimiert. Letzteres unterliegt regelmäßigen und automatisierten Prüfroutinen. Die Frequenz richtet sich auch hier nach der Klassifizierung der Vertraulichkeitsstufe.

Zudem werden bei den AZiD Gesellschaften Verarbeitungstätigkeiten in einem Verzeichnis erfasst, um Transparenz über Verarbeitungsabläufe und Empfänger zu schaffen.

Die Weitergabe von personenbezogenen Daten an unbefugte Dritte ist bei den AZiD Gesellschaften untersagt.

2.2.2 Eingabekontrolle

Um die Überprüfbarkeit und Nachvollziehbarkeit von Dateneingaben, Datenveränderungen und/oder Datenlöschungen sicherzustellen, werden die Zugriffe mit Hilfe von Logdateien protokolliert.

Sicherheitsrelevante Ereignisse (z. B. fehlgeschlagene Loginversuche) werden automatisiert überwacht und ausgewertet.

Der Zugriff auf Systeme und Applikationen wird berechtigten Benutzern nur nach entsprechender Legitimation gewährt. Die Einräumung von Zugangsberechtigungen muss durch Vorgesetzte bzw. Informationseigentümer genehmigt und anschließend auch laufend kontrolliert werden.

Automatisierte oder manuelle Löschroutinen sind in Prozessen in Abstimmung mit dem Datenschutz der AZiD Gesellschaften implementiert.

2.3 Verfügbarkeitskontrolle und Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.3.1 Verfügbarkeitskontrolle

Die AZiD Gesellschaften stellen über arbeitstägliche Datensicherungen die grundsätzliche Verfügbarkeit der personenbezogenen Daten sicher.

Die Datensicherungsträger werden an einem getrennten Ort aufbewahrt und als Bestandteil der Notfallplanung in einem mehr als 200 km entfernten Backup-Rechenzentrum vorgehalten, um die Verfügbarkeit bei einer Katastrophe sicherzustellen.

Malware-Schutz ist in allen relevanten IT-Systemen implementiert.

2.3.2 Maßnahmen zur Sicherstellung der Belastbarkeit

Netzwerke verschiedener Sicherheitsklassifikation sind mittels Firewall getrennt, um das Eindringen Unbefugter in die IT-Systeme zu verhindern.

Über Notfallpläne, welche regelmäßig getestet werden (Business Continuity Management), stellen die AZiD Gesellschaften die Weiterführung des Geschäftsbetriebs nach einer schwerwiegenden Störung bzw. Katastrophe sicher. Die Rechenzentren verfügen über redundante Stromversorgung.

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

2.4.1 Datenschutz-Management

Neue Anwendungen werden vor dem produktiven Einsatz gemäß den Richtlinien für Datenschutz und Informationssicherheit untersucht. Hierzu gehören insbesondere datenschutzfreundliche Voreinstellungen (privacy by design, privacy by default).

Im laufenden Betrieb überprüft die Informationssicherheit der AZiD Gesellschaften regelmäßig alle Anwendungen, abhängig von der Kritikalität der Anwendung. Dazu werden Code Reviews oder Penetrationstests durchgeführt.

Bestehende Sicherheitskonzepte und Richtlinien werden in regelmäßigen Abständen überprüft und bei Bedarf angepasst.

Die AZiD Gesellschaften wirken mit der gebotenen Sorgfaltspflicht im Sinne des Artikel 5 DSGVO darauf hin, dass alle Personen, die mit der Bearbeitung oder Erfüllung von Aufträgen betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten müssen und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weitergeben oder verwerten dürfen.

Datenschutz- und sicherheitsrechtliche Regelungen sind zentraler Bestandteil der verbindlichen Vorgaben für Mitarbeitende im Unternehmen.

Je nach Kritikalität der Verarbeitung personenbezogener Daten nehmen Mitarbeitende an Schulungen zur Informations- und Datensicherheit teil.

Mitarbeitende verpflichten sich auf das Datengeheimnis der Vertraulichkeit und Arbeitsergebnisse werden stets kontrolliert.

2.4.2 Incident Response Management

Die Systeme der Allianz sind durch Firewalls, Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) abgesichert.

Incidents oder bekannt gewordene Schwachstellen werden im CERT der Allianz untersucht und bearbeitet.

Ein SIEM-System (Security Information and Event Management) ist etabliert.

Ein Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen ist dokumentiert und etabliert. Weiterhin existiert ein Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Spamfilter und Malware-Scanner sind im Einsatz und werden regelmäßig aktualisiert.

2.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Eine einfache Ausübung des Widerrufrechts des Betroffenen ist durch technische Maßnahmen gewährleistet.

2.4.4 Weitere Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Bei neuen Anwendungen ist die Durchführung eines Penetrationstest obligatorisch. Bestehende Anwendungen werden abhängig von ihrer Kritikalität jährlich bzw. alle zwei Jahre einem Penetrationstest unterzogen. Bei sicherheitsrelevanten Änderungen an einer Anwendung wird ein außerplanmäßiger Penetrationstest durchgeführt.

Wiederanlauftests und Notfalltests werden regelmäßig durchgeführt.

Business Continuity Test und Krisenstabsübung werden regelmäßig durchgeführt.

2.4.5 Auftragskontrolle / Weisungskontrolle

Die Auswahl und Anbindung der Dienstleister zur Auftragsverarbeitung wird über zentral geregelte Einkaufsprozesse beauftragt.

Die AZiD Gesellschaften stellen gemäß der Auftragskontrolle sicher, dass im Zuge von Verarbeitungstätigkeiten ausschließlich notwendige Daten für die angewiesenen Aufträge verarbeitet werden.

Informationssicherheits- und datenschutzrechtliche Regelungen u. a. in Bezug auf ordnungsgemäße Prozesse in Hinblick auf alle damit verbundenen und angewiesenen Verarbeitungstätigkeiten inkl. Kontrollrechten werden über entsprechende Verträge und Sicherheitskonzepte gewährleistet.

Es erfolgt eine regelmäßige Überprüfung der Auftragsverarbeiter.

Die AZiD Gesellschaften haben einen Datenschutzbeauftragten bestellt.