Vereinbarung zur Auftragsverarbeitung

zwischen

der **xbAV AG**
Arnulfstraße 126, 80636 München
(im Weiteren auch „**Auftragsverarbeiter**“[1] genannt)

und

dem Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO, der den Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten auf der xbAV-Plattform beauftragt
(im Weiteren auch „**Auftraggeber**“ genannt)

[1] Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Bezeichnungen gelten gleichermaßen für beide Geschlechter.

Präambel

Diese Vereinbarung zur Auftragsverarbeitung unterliegt den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) und berücksichtigt insbesondere die Anforderungen nach Art. 28, 32 DSGVO. Die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung gehen hinsichtlich des Umgangs mit personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DSGVO den Bestimmungen des Hauptvertrages vor.

§ 1 Gegenstand des Auftrags

(1) Der Auftragsverarbeiter betreibt eine Plattform im Bereich der betrieblichen Altersversorgung („**bAV**“) als „Software-as-a-Service“ (SaaS) (nachfolgend „**xbAV-Plattform**“ genannt). Die Nutzung der xbAV-Plattform ist in den Allgemeinen Geschäftsbedingungen für die Nutzung der xbAV-Plattform („**Hauptvertrag**“) festgelegt. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO gestützt auf die vorliegende Vereinbarung. Bei den personenbezogenen Daten handelt es sich insbesondere um Daten im Zusammenhang mit der betrieblichen Altersversorgung („**bAV**“) der Arbeitnehmer des Auftraggebers (bei Arbeitgeberkunden) bzw. der Kunden des Auftraggebers (bei Versicherungsvermittlern, Ausschließlichkeitsvermittlern, Versicherungsmaklern etc.).

(2) Der Auftraggeber hat den Auftragsverarbeiter im Rahmen seiner Sorgfaltspflichten gemäß Art. 28, 32 DSGVO ausgewählt.

(3) Der Auftraggeber ist Verantwortlicher der Daten im Sinne von Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Falls erforderlich, hat der Auftraggeber die Betroffenen über die Datenverarbeitung zu informieren oder entsprechende Einwilligungen einzuholen.

(4) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt, sofern der Auftraggeber dem Auftragsverarbeiter nicht eine Verarbeitung in einem Land außerhalb der EU und des EWR gestattet.

(5) Der Auftragsverarbeiter entwickelt die Funktionalitäten der xbAV-Plattform fortwährend weiter, um diese zum Zweck der Erfüllung seiner vertraglichen Pflichten zu verbessern. Sofern in diesem Rahmen neue Funktionalitäten der xbAV-Plattform entwickelt werden und dies zu einer erweiterten Verarbeitung der Daten des Auftraggebers führt, gilt diese erweiterte Datenverarbeitung als von der vorliegenden Vereinbarung umfasst, sobald der Auftraggeber die verbesserten bzw. neuen Funktionalitäten nutzt.

§ 2 Art der verarbeiteten Daten und Kreis der von der Datenverarbeitung Betroffenen

Die im Auftrag zu verarbeitenden, personenbezogenen Daten und die von der Datenverarbeitung Betroffenen sind in **Anlage 1** aufgeführt.

§ 3 Art und Sicherung des Datentransfers

Im Rahmen der Datenverarbeitung innerhalb der xbAV-Plattform nutzt der Auftragsverarbeiter eine dem Stand der Technik entsprechende Verschlüsselungstechnologie. Personenbezogene Daten, die ausnahmsweise auf Weisung des Auftraggebers außerhalb der xbAV-Plattform übertragen werden, sind mit einer risikoadäquaten Sicherung zu versehen (beispielsweise in Form einer verschlüsselten ZIP-Datei).

§ 4 Löschung von Daten

(1) Personenbezogene Daten (unabhängig von ihrer Verkörperung) werden nach Beendigung des Hauptvertrages und Ablauf der gesetzlichen und nachvertraglichen Speicher- und Aufbewahrungsfristen aus allen Speichersystemen des Auftragsverarbeiters gelöscht. Unmittelbar nach Beendigung des Hauptvertrages werden die Daten bis zu ihrer vollständigen Löschung automatisch gesperrt. Der Auftragsverarbeiter ist insbesondere berechtigt, Dokumentationen über Datenverarbeitungsvorgänge innerhalb der Verjährungsfristen etwaiger Schadensersatz- oder Gewährleistungsansprüche Dritter gegen den Auftragsverarbeiter oder den Auftraggeber zu Beweiszwecken aufzubewahren.

(2) Die Löschung wird vom Auftragsverarbeiter dokumentiert. Die Dokumentation über die Löschung wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

§ 5 Allgemeine Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers. Weisungen werden in der Regel durch Bedienung der xbAV-Plattform erteilt. Im Übrigen sind Weisungen oder Zustimmungen des Auftraggebers zu einer von dieser Vereinbarung abweichenden oder darüberhinausgehenden Verarbeitung in Textform (E-Mail genügt) oder in elektronischem Format zu erteilen.

(2) Der Auftragsverarbeiter wird die vom Auftraggeber überlassenen oder für den Auftraggeber erhobenen Daten nicht zu eigenen Zwecken verarbeiten oder nutzen, es sei denn, der Auftraggeber oder Betroffene ist mit einer entsprechenden Verarbeitung oder Nutzung einverstanden.

(3) Der Auftragsverarbeiter ist berechtigt, Arbeitnehmern auf Anfrage die sie betreffenden Daten für die Nutzung der für Arbeitnehmer verfügbaren Funktionalitäten der xbAV-Plattform (insbesondere: Arbeitnehmer-Zugang) zur Verfügung zu stellen.

(4) Der Auftragsverarbeiter bestätigt, dass er den in **Anlage 2** benannten betrieblichen Datenschutzbeauftragten i.S.v. Art. 37 Abs. 1 DSGVO bestellt hat. Ein etwaiger Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich angezeigt. Der Auftragsverarbeiter stellt dem Auftraggeber die Prüfberichte des Datenschutzbeauftragten im Hinblick auf das Auftragsverhältnis auf Anfrage zur Verfügung.

(5) Der Auftragsverarbeiter ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor einer unbefugten Kenntnisnahme Dritter geschützt sind, wie in den „Technischen und organisatorischen Maßnahmen“ (**Anlage 3**) aufgeführt.

(6) Der Auftragsverarbeiter verpflichtet sich ferner, eine adäquate Dokumentation der Datenverarbeitung zu führen, anhand derer der Auftraggeber deren Ordnungsmäßigkeit feststellen kann.

(7) An der Erstellung von Datenschutzfolgeabschätzungen durch den Auftraggeber wird der Auftragsverarbeiter, soweit rechtlich erforderlich, mitwirken.

§ 6 Gegenseitige Hinweispflichten der Vertragspartner, Prüfungen der Aufsichtsbehörden

(1) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO, das BDSG oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(2) Bei der Verletzung des Schutzes von vom Auftraggeber überlassenen oder für den Auftraggeber erhobenen Daten durch den Auftragsverarbeiter ist der Auftraggeber unverzüglich zu informieren. Dies gilt insbesondere im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter wird den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und Art. 34 DSGVO angemessen unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Falls nach Einschätzung des Auftragsverarbeiters von der vorliegenden Vereinbarung erfasste

a) besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), oder

b) personenbezogene Daten, die einem Berufsgeheimnis unterliegen, oder

c) personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder

d) personenbezogene Daten zu Bankkonten oder Kreditkarten

unrechtmäßig an Dritte übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle und Art der unrechtmäßigen Kenntniserlangung zu informieren.

(3) Soweit Prüfungen der Datenschutzaufsichtsbehörden beim Auftraggeber stattfinden, die die vorliegende Vereinbarung betreffen, verpflichtet sich der Auftragsverarbeiter, den Auftraggeber im Rahmen der vorliegenden Vereinbarung auf Anfrage zu unterstützen. Die Vertragspartner verpflichten sich, bei Prüfungen der Datenschutzaufsichtsbehörden festgestellte Mängel, welche aus dem vorliegenden Vertragsverhältnis resultieren bzw. dieses beeinflussen, unverzüglich abzustellen. Die jeweiligen Kosten sind von demjenigen Vertragspartner zu tragen, der die Mängel zu vertreten hat.

(4) Die Parteien werden sich gegenseitig schnellstmöglich über Kontrollhandlungen und Maßnahmen der Datenschutzaufsichtsbehörde informieren, soweit sie die vorliegende Vereinbarung betreffen. Dies gilt auch, wenn eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten in Zusammenhang mit der vorliegenden Vereinbarung bei einer Partei ermittelt.

§ 7 Vertraulichkeit

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Mitarbeiter zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO).

(2) Beauftragte Dritte, die nicht Mitarbeiter des Auftragsverarbeiters sind, wird der Auftragsverarbeiter im selben Umfang, wie er selbst gegenüber dem Auftraggeber verpflichtet ist, zur Vertraulichkeit, Geheimhaltung und zum Datenschutz verpflichten und dies dem Auftraggeber auf Verlangen nachweisen.

§ 8 Auftragsmaterial: Herausgabe, Entsorgung

(1) Der Hauptvertrag und die vorliegende Vereinbarung beziehen sich auf die digitale Nutzung von Funktionalitäten auf der xbAV-Plattform. Daten werden demnach in der Regel digital verarbeitet, ausgetauscht und gespeichert und durch digitale Sicherheitssysteme beim Auftragsverarbeiter geschützt.

(2) Soweit Daten im Rahmen der vorliegenden Vereinbarung in anderer Form verarbeitet, ausgetauscht oder aufbewahrt werden, kennzeichnet der Auftragsverarbeiter Unterlagen und Datenträger mit Daten des Auftraggebers, bewahrt sie getrennt von seinen Unterlagen und Daten auf und schützt sie durch geeignete Maßnahmen gegen den Zugriff Unberechtigter sowie gegen nicht vertragsgemäße Nutzung, Vervielfältigung und Weitergabe.

(3) Bei Beendigung des Hauptvertrages gibt der Auftragsverarbeiter dem Auftraggeber die erhaltenen Unterlagen und Datenträger auf Anfrage heraus oder weist dem Auftraggeber deren ordnungsgemäßen Vernichtung nach.

§ 9 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter ist berechtigt, zum Zweck der Erfüllung dieses Vertrages Unterauftragsverarbeiter zu beauftragen. Alle zum Zeitpunkt des Vertragsschlusses bestehenden Unterauftragsverhältnisse sind in **Anlage 4** genannt. Die Liste der Unterauftragsverarbeiter wird auf der xbAV-Plattform laufend aktualisiert.

(2) Der Auftraggeber wird während der Vertragslaufzeit vom Auftragsverarbeiter über jede bevorstehende Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in Textform (E-Mail genügt) oder in elektronischem Format spätestens 6 Wochen vor der geplanten Hinzuziehung oder Ersetzung des jeweiligen Unterauftragsverarbeiters informiert. Die Information enthält den beabsichtigen Zeitpunkt der Hinzuziehung oder Ersetzung des Unterauftragsverarbeiters („**Umsetzungszeitpunkt**"), einen Hinweis auf das Widerspruchs- und Kündigungsrecht des Auftraggebers und einen Hinweis darauf, dass der Auftraggeber der Hinzuziehung bzw. Ersetzung des Unterauftragsverarbeiters zustimmt, wenn er nicht bis zum Umsetzungszeitpunkt widerspricht. Der Auftraggeber hat die Möglichkeit bis zum Umsetzungszeitpunkt in Textform (E-Mail genügt) oder in elektronischem Format zu widersprechen. Macht der Auftraggeber von seinem Widerspruchsrecht bis zum Umsetzungszeitpunkt Gebrauch, haben beide Vertragsparteien das Recht, das Vertragsverhältnis ab dem Zeitpunkt des Zugangs des Widerspruchs beim Auftragsverarbeiter innerhalb von 30 Tagen mit einer Frist von 14 Tagen zu kündigen. Wenn der Auftraggeber von seinem Widerspruchsrecht nicht bis zum Umsetzungszeitpunkt Gebrauch macht, gilt dies als Zustimmung zur Hinzuziehung oder Ersetzung des jeweiligen Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter hat Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung sicherzustellen, dass die Unterauftragsverarbeiter die zwischen Auftraggeber und Auftragsverarbeiter getroffenen Vereinbarungen einhalten. Der Auftragsverarbeiter hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Die Verpflichtung des Unterauftragsverarbeiters erfolgt schriftlich oder in elektronischem Format.

§ 10 Nachvertragliche Pflichten des Auftragsverarbeiters

(1) Im Fall einer Schadenersatzforderung, insbesondere gemäß Art. 82 DSGVO, bzw. eines Bußgeldes, insbesondere gemäß Art. 83 DSGVO oder gemäß Art. 84 DSGVO, wegen behaupteter unzulässiger oder unrichtiger Datenverarbeitung hat der Auftragsverarbeiter dem Auftraggeber die vorhandene Dokumentation zur Führung des Entlastungsbeweises auch nach Vertragsende auf Anfrage zur Verfügung zu stellen, soweit diese vom Auftragsverarbeiter nicht pflichtgemäß gelöscht wurde.

(2) Ferner ist der Auftragsverarbeiter verpflichtet, den Auftraggeber anlässlich der Verletzung von Datenschutzbestimmungen, die die Auftragsdaten aus diesem Vertrag betreffen, auch nach Beendigung des Vertrages unverzüglich zu benachrichtigen.

§ 11 Wahrung von Betroffenenrechte

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte grundsätzlich allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragsverarbeiters für die Wahrung der Betroffenenrechte nach Art. 12 - 22 DSGVO - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragsverarbeiter die jeweils notwendigen Maßnahmen nach Weisung des Auftraggebers treffen, um den Auftraggeber zu unterstützen.

(3) Der Auftragsverarbeiter wird den Auftraggeber insbesondere bei der Wahrung der Betroffenenrechte auf Datenportabilität (Art. 20 DSGVO) unterstützen. Der Auftragsverarbeiter wird dem Auftraggeber entsprechend einzelne Datensätze von Betroffenen auf Anfrage innerhalb angemessener Frist (in der Regel innerhalb von drei Wochen) in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragsverarbeiter entstehen, bleiben unberührt.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragsverarbeiter Bestimmungen der vorliegenden Vereinbarung oder gesetzliche Bestimmungen zu Datenschutz oder Datensicherheit vorsätzlich oder grob fahrlässig verletzt. Bei einfachen Verstößen setzt der Auftraggeber dem Auftragsverarbeiter zunächst eine angemessene Nachfrist, um Abhilfe zu schaffen.

(2) Nachvertragliche Verpflichtungen gemäß der vorliegenden Vereinbarung bleiben hiervon unberührt.

§ 13 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann sich gemäß Art. 28 Abs. 3 lit. h DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit dieser Vereinbarung von der Einhaltung der beim Auftragsverarbeiter eingerichteten technischen und organisatorischen Maßnahmen gemäß **Anlage 3** zur vorliegenden Vereinbarung überzeugen. Vom Auftraggeber oder einem von ihm beauftragten Prüfer durchgeführte Überprüfungen wird der Auftragsverarbeiter ermöglichen und, sofern erforderlich, zu ihrer Durchführung beitragen.

(2) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist vor-Ort Kontrollen an den Betriebsstätten des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei den zeitlichen und quantitativen Umfang von vor-Ort Kontrollen so effektiv wie möglich gestalten und vor-Ort Kontrollen nur im erforderlichen Umfang durchführen.

(3) Durch Überprüfungen und vor-Ort Kontrollen entstehende Kosten hat der Auftraggeber zu tragen; dies umfasst eine branchenübliche Aufwandsentschädigung für die Arbeitszeit des vom Auftragsverarbeiter beanspruchten Personals.

(4) Der Auftraggeber hat bei Überprüfungen und vor-Ort Kontrollen sicherzustellen, dass Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters von ihm, seinen Mitarbeitern und von ihm beauftragten Prüfern gewahrt werden.

§ 14 Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragsverarbeiter gewährleistet die Einhaltung der im Rahmen der vertragsgegenständlichen Tätigkeiten erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Diese Maßnahmen sind in **Anlage 3** dokumentiert. Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt Auditbericht wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

§ 15 Schlussbestimmungen

(1) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages. Sie endet ohne Weiteres mit Beendigung des Hauptvertrages.

(2) Der Auftraggeber wird während der Vertragslaufzeit vom Auftragsverarbeiter über jede bevorstehende Änderung dieser Vereinbarung in Textform (E-Mail genügt) oder in elektronischem Format spätestens 6 Wochen vor der geplanten Änderung informiert. Die Information enthält den beabsichtigen Zeitpunkt der Änderung („**Umsetzungszeitpunkt**"), einen Hinweis auf das Widerspruchs- und Kündigungsrecht des Auftraggebers und einen Hinweis darauf, dass der Auftraggeber der Änderung zustimmt, wenn er nicht bis zum Umsetzungszeitpunkt widerspricht. Der Auftraggeber hat die Möglichkeit bis zum Umsetzungszeitpunkt in Textform (E-Mail genügt) oder in elektronischem Format zu widersprechen. Macht der Auftraggeber von seinem Widerspruchsrecht bis zum Umsetzungszeitpunkt Gebrauch, haben beide Vertragsparteien das Recht, die vorliegende Vereinbarung und den Hauptvertrag ab dem Zeitpunkt des Zugangs des Widerspruchs beim Auftragsverarbeiter innerhalb von 30 Tagen mit einer Frist von 14 Tagen zu kündigen. Wenn der Auftraggeber von seinem Widerspruchsrecht nicht bis zum Umsetzungszeitpunkt Gebrauch macht, gilt dies als Zustimmung zur Änderung dieser Vereinbarung.

(3) Mitteilungen im Rahmen dieser Vereinbarung erfolgen in Schriftform (E-Mail genügt) oder in elektronischer Form.

(4) Die dieser Vereinbarung beigefügten **Anlagen 1 bis 4** sind Bestandteil dieser Vereinbarung zur Auftragsverarbeitung.

Anlage 1 zur AV

Zweck der Datenerhebung, -verarbeitung und -nutzung

Zweck der Datenerhebung, -verarbeitung und -nutzung ist die Nutzung der xbAV-Plattform durch den Auftraggeber. Damit verbunden ist die Verarbeitung von bAV-Daten der Arbeitnehmer bzw. Kunden des Auftraggebers durch den Auftragsverarbeiter.

Von der Auftragsverarbeitung umfasste Leistungen

- Von der Auftragsverarbeitung sind insbesondere folgende Leistungen erfasst (sofern darin personenbezogene Daten enthalten sind):
  - Anzeige von Partner- und Vertragsdaten
  - Verwaltung von Geschäftsvorfällen für Bestands- und Neugeschäft
  - Dokumentenanzeige und Verwaltung
  - Einsicht in laufende Versorgungen
  - Auswahl von Tarifvertragsvorlagen
  - Konfiguration und ggf. Anpassung von Versorgungsordnungsbausteinen und Zuschüssen
  - Konfiguration von Tarifen und Prozessen
  - Kommunikation von Fehlermeldungen
  - Automatische Anlage und Aktualisierung von Arbeitnehmern
  - Einladung von Arbeitnehmern zum Arbeitnehmerzugang und zur Nutzung des Arbeitnehmerportals
  - Zuordnung von Arbeitnehmern zu Versorgungsbausteinen und damit verbundene Erzeugung von Anträgen
  - Freigabe von durch Arbeitnehmer erstellten Anträgen
  - Nutzung der elektronischen Unterschrift
  - Antragsübermittlung an den Produktanbieter
  - Darstellung von Rentenlücken und Zuschüssen
  - Ermöglichung von Selbstinformation und Schnellberechnungen
  - Verwaltung von Beratungswünschen
  - Analyse von Daten zur Verbesserung der User Experience
- Dem Auftragsverarbeiter ist auch die Anonymisierung von Daten und die Verwendung von aggregierten Daten erlaubt, u.a. zur Erstellung anonymer Auswertungen, Statistiken und Prozesse zur Auswertung und Verbesserung der Funktionalitäten der xbAV-Plattform.

Folgende Daten sind regelmäßig Gegenstand der Datenverarbeitung

- Daten der Arbeitnehmer des Auftraggebers (bei Arbeitgeberkunden) bzw. der Kunden des Auftraggebers (bei Versicherungsvermittlern, Ausschließlichkeitsvermittlern, Versicherungsmaklern etc.) wie beispielsweise
  - Vertrags-/Stamm- und Abrechnungsdaten, einschließlich Daten zur Lohn- und Gehaltsabrechnung, zur Lohnsteuer und Sozialversicherung; Angaben zum Tätigkeitsbereich; Name und Alter von Angehörigen (einschließlich Notfallkontaktdaten bei Verhinderung des Arbeitnehmers), soweit diese Daten für Versicherungs- oder Sozialleistungen relevant sind; Bankverbindungsdaten; Arbeitnehmerstatus;
  - Falls erforderlich Gesundheitsdaten (beispielsweise zur Berechnung einer Berufsunfähigkeitsversicherung).

Von der Datenverarbeitung Betroffene

Arbeitnehmer des Auftraggebers bzw. Kunden des Auftraggebers.

Kategorien von Empfängern, denen die Daten mitgeteilt werden können

- Versicherungsunternehmen und bAV-Produktanbieter aller Rechtsformen und Durchführungswege einschließlich Versicherungsvereine auf Gegenseitigkeit, Pensionsfonds und Unterstützungskassen.
- Unterauftragsverarbeiter entsprechend Art. 28, 32 DSGVO zur Abwicklung der Verarbeitung der Daten im Auftrag des Auftragsverarbeiters.
- Kreditinstitute, oder andere externe Stellen zur Erfüllung der oben genannten Zwecke, sofern der Betroffene entweder seine Einwilligung in Textform (E-Mail genügt) oder in elektronischem Format erklärt hat, dies zur Vertragserfüllung erforderlich oder eine Übermittlung aus überwiegendem berechtigtem Interesse zulässig ist.

Anlage 2 zur AV

Externer Datenschutzbeauftragter

xbAV AG
Konstantin Pflüger
Arnulfstr. 126
80636 München
datenschutz@xbav.de
Fon: +49 (0) 89 2000 17-50
Fax: +49 (0) 89 2000 17-99

Der Empfang von E-Mails kann aus technischen oder betrieblichen Gründen in Ausnahmefällen gestört sein. Bitte stellen Sie sicher, dass zeitkritische Nachrichten zusätzlich auf dem Postweg oder via Telefax übermittelt werden. Bitte bedenken Sie, dass die Kommunikation per E-Mail grundlegend unsicher ist, da die Möglichkeit der Kenntnisnahme und Manipulation durch Dritte besteht. Vertrauliche Daten sollten keinesfalls unverschlüsselt per E-Mail übermittelt werden.

Anlage 3 zur AV

Technische und organisatorische Maßnahmen (TOM)

Ziel

Dieses Dokument beschreibt den aktuellen Stand der beim Auftragsverarbeiter umgesetzten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g DSGVO) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d DSGVO). Der Grad der Detaillierung ist an dieser Stelle bewusst geringgehalten. Nähere Ausführungen sind im internen Sicherheitskonzept des Auftragsverarbeiters enthalten. Ein Zugang zum Sicherheitskonzept wird auf Anfrage in geeigneter Form durch den Auftraggeber gewährt.

Allgemeine Maßnahmen

Die technischen und organisatorischen Maßnahmen werden durch den internen Datensicherheitsbeauftragten und den Datenschutzbeauftragten in regelmäßigen Abständen überprüft und dem Schutzbedarf bzw. dem Stand der Technik angepasst.

Prüfungen werden protokolliert.

Der Auftragsverarbeiter hat geeignete Prozesse und Leitlinien für die Einhaltung der Verhaltensregeln nach Art. 40 DSGVO umgesetzt.

Es werden die wichtigsten Newsfeeds (CERT, OWASP, Heise Security, BSI) durch das Security Team des Auftragsverarbeiters gelesen und durch den internen Datensicherheitsbeauftragten bewertet. Auf daraus resultierende neue Anforderungen wird mit einem konkreten Maßnahmenkatalog reagiert und im internen Sicherheitskonzept dokumentiert.

Für die regelmäßige Überprüfung der Verwundbarkeit des xbAV-Plattform werden geeignete Überwachungstools eingesetzt. Dabei wird durch den internen Datensicherheitsbeauftragten eine jeweils aktuelle Evaluation der verfügbaren Werkzeuge durchgeführt und mit dem Datenschutzbeauftragten abgestimmt.

Die Ergebnisse werden dokumentiert. Ergibt sich aus einer Prüfung Handlungsbedarf, leitet der interne Datensicherheitsbeauftragte adäquate Maßnahmen ein.

Pseudonymisierung und Verschlüsselung

- Verschlüsselung der Daten (auf Kommunikations- und Persistenzebene).
- Testsysteme und Entwicklungsumgebungen enthalten keine Echtdaten.
- Testdaten werden synthetisch erzeugt oder es handelt sich um anonymisierte Daten.

Vertraulichkeit

- Alle Mitarbeiter sind zur Vertraulichkeit verpflichtet.
- Datenträger und Papierakten mit personenbezogenen Daten werden durch einen zertifizierten Dienstleister vernichtet.
- Es besteht ein elektronisches Zutrittskontrollsystem.
- Es existieren Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude.
- Es besteht Videoüberwachung an den Ein- und Ausgängen der Betriebsstätten des Auftragsverarbeiters.
- Es erhalten nur selektive Mitarbeiter des Auftragsverarbeiters Zugang zur xbAV-Plattform und zu Produktivdaten. Dieser Zugang ist elektronisch abgesichert.
- Es erfolgt eine datenschutzkonforme Löschung der Daten nach Auftragsbeendigung und Ablauf der Aufbewahrungs- bzw. Speicherfristen.
- Es existiert ein verbindliches Rollen- und Berechtigungskonzept für Mitarbeiter des Auftragsverarbeiters.
- Backups werden vor unbefugtem Zugriff gesichert.
- Die Übertragung von personenbezogenen Daten auf externe Datenträger ist Mitarbeitern des Auftragsverarbeiters verboten.

Integrität

- Es sind geeignete Systeme zum Schutz vor Schadprogrammen installiert.
- Es existiert ein Virenschutz auf Arbeitsplatzebene und bei Serversystemen.
- Virendefinitionen werden täglich erneuert.

Belastbarkeit

- Es wurden technische Vorkehrungen getroffen, um DoS und DDoS Attacken zu verhindern.
- Es werden regelmäßige Lasttests durchgeführt.

Verfügbarkeit

- Es finden regelmäßige Updates statt.
- Es findet ein sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) statt.
- Das Betriebskonzept der xbAV-Plattform enthält adäquate Redundanzmechanismen.
- Es wird eine unterbrechungsfreie Stromversorgung eingesetzt.
- Es existiert ein Backup- und Recovery-Konzept mit täglicher Sicherung der Daten auf physikalisch getrennten Volumes.
- Es findet eine Verschlüsselung der Backups statt.
- Es werden Softwarefirewall und Portreglementierungen eingesetzt.

Anlage 4 zur AV

Unterauftragsverarbeiter

Der Auftragsverarbeiter ist berechtigt, für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch zu nehmen, die in seinem Auftrag Daten verarbeiten („**Unterauftragsverarbeiter**“).

Dabei handelt es sich derzeit um folgende Unternehmen:

1. **xbAV Beratungssoftware GmbH** — Softwareentwicklung
   Arnulfstr. 126
   80636 München
   Tel.: 0681 210 738-0
   Fax: 0681 210 738-99
   E-Mail: info@xbav-berater.de
   Handelsregister: Amtsgericht München, HRB 217016
   USt-IdNr.: DE 301 576 735

2. **The unbelievable Machine Company GmbH** — Hosting-Unternehmen
   Grolmanstr. 40
   10623 Berlin
   Tel.: 030 8892656-0
   Fax: 030 8892656-11
   E-Mail: info@unbelievable-machine.com
   Handelsregister: Amtsgericht Charlottenburg, HRB 115071
   USt-IdNr.: DE 261090159

3. **documentus Bayern GmbH** — Aktenvernichter – Entsorgungsfachbetrieb
   Ziegeleistraße 13
   86368 Gersthofen
   Tel.: 0821 29776-0
   Fax: 0821 29776-50
   E-Mail: info@documentus-bayern.de
   Handelsregister: Amtsgericht Augsburg, HRB 10622
   USt-IdNr.: DE 127495424

4. **documentus GmbH Saarbrücken** — Aktenvernichter – Entsorgungsfachbetrieb
   Behrener Straße 10
   66117 Saarbrücken
   Tel.: 0681 93 52 14-0
   Fax: 0681 93 52 14-40
   E-Mail: info@documentus-sb.de
   Handelsregister: Amtsgericht Saarbrücken, HRB 8869
   USt-IdNr.: DE 138 111 334

5. **salesforce.com Germany GmbH** — CRM-Plattform
   Erika-Mann-Str. 31
   80636 München
   Tel.: 0800 1822338
   E-Mail: info-de@salesforce.com
   Handelsregister: Amtsgericht München, HRB 158525
   USt-IdNr.: DE 245335078

6. **Binect GmbH** — Postversanddienstleister
   Robert-Koch-Str. 9
   64331 Weiterstadt
   Tel.: 06151 9067-0
   Fax: 06151 9067-291
   E-Mail: info@binect.de
   Handelsregister: Amtsgericht Darmstadt, HRB 94685
   USt-IdNr.: DE 22130226