Vereinbarung zur Auftragsverarbeitung

(Datenschutz gemäß Art. 28 DS-GVO)

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

AEB SE

Sigmaringer Straße 109, D-70567 Stuttgart

- Auftragsverarbeiter - nachstehend Auftragnehmer oder AEB genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

.....]

Inhalt

1 Präambel

1.1 Vorbemerkungen der AEB

Die AEB möchte den Anforderungen zur datenschutzrechtlichen Regelung der Auftrags(daten)verarbeitung gerecht werden. Für einen möglichst reibungslosen Vertragsprozess ist diesem Vertragswerk die Mustervorlage sowohl der BITKOM (Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)) als auch der GDD zugrunde gelegt. Einzelne Anpassungen sind hier eingearbeitet.

1.2 Präambel Bitkom

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der in der Leistungsvereinbarung beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

2 Gegenstand, Dauer und Konkretisierung der Auftragsverarbeitung

2.1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung (im Folgenden Leistungsvereinbarung).

Die Leistungsvereinbarung ergibt sich aus Aufträgen zu Leistungen des Auftragnehmers. Die Leistungen umfassen

- Erteilung zur Nutzung von durch AEB angebotenen Software-Lösungen
- Services (wie z.B. Support, Hosting).

Diese Aufträge/Verträge der Leistungsvereinbarung sind beiden Parteien bekannt. Auf Anfrage des Auftraggebers kann AEB dem Auftraggeber die Verträge bzw. betroffenen Lösungsbereiche in Listen-Form zukommen lassen. Die Liste kann einvernehmlich erweitert/geändert werden. Beide Parteien beachten mögliche Auswirkungen dieser Erweiterungen/Änderungen auf den vorliegenden Vertrag zur Auftragsverarbeitung.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Die Wirksamkeit dieses Vertrags beginnt am 25. Mai 2018.

Etwaige bestehende frühere Vereinbarungen zum Datenschutz zur Regelung der Auftrags(daten)verarbeitung werden mit dem Wirksamwerden dieses Vertrags durch diesen Vertrag abgelöst.

2.2 Konkretisierung des Auftrags(inhalts)

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Wenn nicht anders angegeben, besteht der Zweck der Verwendung personenbezogener Daten in der Hinterlegung eines Sachbearbeiters (mit Name, Kontakt) in Vorgängen der Software-Lösungen, etwa zu Zwecken der Rücksprache-Möglichkeit.

Der Einsatz der Applikation Compliance zum Screening von Adressen gegen Sanktionslisten/Anti-Terrorlisten dient der Herstellung von Rechtskonformität im Umfeld von einschlägigen Antiterrorverordnungen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Voraussetzung für eine zulässige Leistungserbringung der AEB an Orten außerhalb des oben beschriebenen Raumes (Beispiel: Schweiz) ist ein angemessenes Schutzniveau. Zulässige Möglichkeiten sind: Das angemessene Schutzniveau…

- ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner

3 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsvereinbarung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Dem Auftragnehmer (»Auftragsverarbeiter« im Sinne des Art. 4 Nr. 8 DS-GVO) erwachsen Pflichten gemäß Art. 28 DS-GVO.

4 Pflichten des Auftragnehmers

4.1 Weisungsgebundenheit

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

4.2 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(2) Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in **Anhang 1**].

(3) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(5) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(6) Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf vorliegende Zertifizierungen (und ggf. weitere Zertifikate) zu Datenschutz oder Informationssicherheit verwiesen, mit deren Vorlage der Nachweis geeigneter Garantien erbracht werden kann.

4.3 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Der Auftraggeber übernimmt die dabei anfallenden Kosten.

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht in anderen Verträgen bereits vereinbart.

4.4 Sonstige Pflichten zur Unterstützung

(1) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Aufwände, die dem Auftragnehmer bei der Wahrnehmung dieser Pflichten entstehen, werden ihm durch den Auftraggeber ab Übersteigen eines üblichen Aufwandes (= bis zu 4 Personenstunden je Jahr) nach dem geltenden Stundensatz des Auftragnehmers erstattet.

(2) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(3) Der Auftragnehmer nennt dem Auftraggeber seinen Datenschutzbeauftragten als Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Sein Kontakt: datenschutzbeauftragter@aeb.com. Die aktuellen Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(4) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Entstehen zusätzliche Kosten durch abweichende bzw. bisher nicht festgelegte Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne Art. 30 DS-GVO.

(6) Der Auftragnehmer führt geeignete Maßnahmen zur Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durch. Er unterstützt den Auftraggeber mit entsprechenden Informationen, insbesondere über die Ergebnisse der Abschätzung, soweit Verfahren der hier zugrundeliegenden Auftragsverarbeitung betroffen sind.

(7) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Aufwände, die dem Auftragnehmer bei der Wahrnehmung dieser Pflichten entstehen, werden ihm durch den Auftraggeber ab Übersteigen eines üblichen Aufwandes (= bis zu 4 Personenstunden je Jahr) nach dem geltenden Stundensatz des Auftragnehmers erstattet.

(8) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(9) Der Auftragnehmer informiert unverzüglich den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(10) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(11) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

5 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Abschnitt 4.4 Abs. (7) entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

6 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

7 Kontrollen und Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer dem Auftraggeber folgende Informationen zur Verfügung stellen und vorlegen:

- Durchführung eines Selbstaudits
- Zertifikat zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001)
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Genehmigte Verhaltensregeln nach Art. 40 DS-GVO
- Zertifikate nach Art. 42 DS-GVO

(3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen

Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Aufwände, die dem Auftragnehmer für die Unterstützung bei der Durchführung einer Inspektion entstehen, werden ihm durch den Auftraggeber ab Übersteigen eines üblichen Aufwandes (= bis zu 4 Personenstunden je Jahr) nach dem geltenden Stundensatz des Auftragnehmers erstattet.

(5) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 4 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

8 Subunternehmer (weitere Auftragsverarbeiter)

(1) 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-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist grundsätzlich nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

Der Auftraggeber stimmt hiermit gemäß Art. 28 Abs. 2 DS-GVO als „allgemeine schriftliche Genehmigung“ zu, dass der Auftragnehmer Subunternehmer hinzuzieht.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name des Subunternehmers	**Beschreibung der Teilleistungen**	**Anschrift**
AFI Solutions GmbH	Wartung und Support zu Software für Middleware (Kommunikationssoftware)	Stuttgart / Deutschland
Trivadis GmbH	Datenbank-Administration und -Support	Stuttgart / Deutschland
Hewlett Packard GmbH	Hardware-Lieferant	Böblingen / Deutschland

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(4) Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist (von 6 Wochen ab Eingang der Information) – aus wichtigem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller hier vereinbarten Voraussetzungen für eine Unterbeauftragung gestattet.

9 Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem

Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung zur Auftragsverarbeitung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen einer Leistungsvereinbarung vor. Sollten einzelne Teile dieser Vereinbarung zur Auftragsverarbeitung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung zur Auftragsverarbeitung im Übrigen nicht.

(4) Es gilt deutsches Recht.

11 Haftung und Schadensersatz

11.1 Allgemeines

Soweit in der Leistungsvereinbarung nicht anders vereinbart, gilt Art. 82 Abs. 2 und Abs. 3 DS-GVO.

11.2 Weitere Regelungen

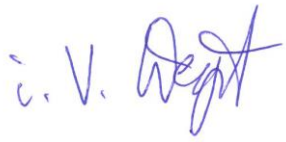
Soweit gesetzlich nicht ausdrücklich anders geregelt muss jeglicher Anspruch dem Grund und der Höhe nach detailliert nachgewiesen werden.

Den Parteien ist bekannt, dass der Auftragnehmer ein Sicherheitskonzept entwickelt hat, durchführt und weiter verbessert. Das Sicherheitskonzept des Auftragnehmers ist dem Auftraggeber zugänglich und wird von diesem durch Unterzeichnung dieses Vertrags als ausreichend abgenommen.

Den Parteien ist ebenso bekannt, dass sich nachträglich einzelne Maßnahmen des Sicherheitskonzepts des Auftragnehmers trotz verkehrsüblicher Sorgfalt als für eine einzelne Situation als nicht ausreichend darstellen könnten. Sollte eine solche Einzelsituation auftreten, so wird diese nicht von den Parteien als Grundlage für die Geltendmachung von Ansprüchen herangezogen werden, weder im Rahmen der Geltendmachung von Vertragsverletzung, noch als Eintritt einer Bedingung für die Auslösung eines Vertragsstrafenanspruchs.

Der Vertrag kommt zustande durch Zeichnung

- des Auftraggebers durch elektronische Bestätigung nach Aufklärung und Aufforderung durch die AEB. Der Auftraggeber erhält daraufhin für seine Unterlagen ein entsprechendes E-Mail zur Empfangsbestätigung.
- des Auftragnehmers wie folgt

Auftragnehmer
Stuttgart Ort
14.01.2019 Datum
Volkher Wegst / Datenschutzbeauftragter Name / Funktion
 Unterschrift

12 Anhänge

12.1 Technische und organisatorische Maßnahmen (Anhang 1)

12.1.1 Beschreibung

Aufstellung der technischen und organisatorischen Maßnahmen; mitwirkendes Dokument zum aktuellen Stand mit Titel: „Datensicherheit bei der AEB Gesellschaft zur Entwicklung von Branchen-Software mbH“.

Die Maßnahmen dürfen und sollen nach **Stand der Technik** fortgeführt werden so, dass das erreichte Datenschutz-Niveau nicht unterschritten wird.

12.1.2 Zum Dokument

Das Dokument zu den technischen und organisatorischen Maßnahmen ist auf dem aktuellen Stand diesem Vertrag als Anhang 1 beigefügt und kann zudem künftig auf Anfrage in der jeweils gültigen Fassung beim Datenschutzbeauftragten zur Verfügung gestellt werden.

Es ist bis auf weiteres auch auf der Web-Seite der AEB unter https://service.aeb.de/open/leitlinien-und-zertifikate/ unter dem Namen **Sicherheitskonzept** verfügbar gemacht.