# Ergänzende Bedingungen zur Auftragsverarbeitung

AEB IT-SYSTEME GmbH

**Inhaltsverzeichnis**

**Präambel**

Ab dem 25.05.2018 ist die EU-Datenschutzgrundverordnung anzuwenden. Dadurch ist eine Anpassung der bestehenden Datenschutzorganisation auch im Hinblick auf Auftragsdatenverarbeitung notwendig. Aus diesem Grund verpflichtet sich AEB IT-SYSTEME GmbH als Auftragsverarbeiter (im Folgenden: „Auftragnehmer“) gegenüber dem Auftraggeber als Verantwortlichen nach Maßgabe von Art. 28 Abs.3 S. 1 Alt.2 DS-GVO wie folgt:

## § 1 Gegenstand und Dauer des Auftrags

Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

1. Datenmigration

    a. Die Prüfung der Daten sowie die Übertragung dieser in ein neues Datenbankformat, sind im Rahmen eines Softwarewechsels und der damit einhergehenden Modernisierung notwendig. Ebenfalls notwendig ist die Übertragung der Daten im Rahmen von Supportfällen zur Prüfung, um Fehler und Inkonsistenzen zu beheben.

2. Fernwartung/Support

    a. Der Support kann telefonisch oder über eine Fernwartungssoftware erfolgen. Im Rahmen des Supports/der Fernwartung werden keine persönlichen Daten übertragen oder gespeichert, sofern diese nicht im Rahmen einer Datenübertragung zu Supportzwecken zu AEB übertragen werden.

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von drei Monaten zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## § 2 Konkretisierung des Auftragsinhalts

1. Die Art der verarbeiteten personenbezogenen Daten sowie die Kategorien der Betroffenen werden in Anlage 1 zu diesen ergänzenden Bedingungen konkretisiert.
2. Die Erbringung der gegenständlichen 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 Art. 44 ff. DS-GVO erfüllt sind.

## § 3 Technisch-organisatorische Maßnahmen

1. 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.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um solche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. 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. Die einzelnen seitens des Auftragnehmers ergriffenen Maßnahmen sind in Anlage 2 zu diesen ergänzenden Bedingungen zur Auftragsverarbeitung aufgeführt.
3. 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.

## § 4 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. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Löschung, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## § 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Tobias Aland (E-Mail an: tobias.aland@aebit.de) benannt.
2. Zur Wahrung der Vertraulichkeit setzt der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten

Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesen ergänzenden Bedingungen zur Auftragsverarbeitung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3. Der Auftragnehmer ist zur Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Anlage 2 dieser ergänzenden Bedingungen verpflichtet.
4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5. Der Auftraggeber ist verpflichtet, den Auftragnehmer über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, 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.
6. 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.
7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieser ergänzenden Bedingungen.

## § 6 Unterauftragsverhältnisse

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. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

3. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

4. Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

5. Sämtliche hier aufgeführten Bedingungen zur Auftragsverarbeitung sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## § 7 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Geschäftsbetrieb des Auftragnehmers Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser ergänzenden Bedingungen zur Auftragsverarbeitung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

2. 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.

3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## § 8 Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zum Schutz personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.

   a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte

Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

## § 9 Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## § 10 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.

**Anlage 1:** **A. Zu § 2 Abs. 1: Art der personenbezogenen Daten**

**B. Zu § 2 Abs. 1: Kreis der Betroffenen**

**Anlage 2:** **Technisch-organisatorische Maßnahmen gemäß Art. 32 DS-GVO**

**Anlage 1:**

**A. Zu § 2 Art der personenbezogenen Daten**

(maßgebliche Datenarten sind angekreuzt)

☒ Adressdaten, ☒ Kontaktdaten, ☐ Vertragsdaten, ☒ Bankverbindungsdaten,☒ Kontodaten ☒ Abrechnungsdaten, ☒ Gesprächshistorie, ☐ Transaktionsdaten, ☒ Auskünfte, ☒ Mitarbeiterdaten, ☐ Personalverwaltung, ☐ Gesundheitsdaten

Andere sensible Daten:

Sonstige:

**B. Zu § 2 Kreis der Betroffenen**

(maßgebliche Personengruppen sind anzukreuzen)

☒ Mitarbeiter, ☒ Praktikanten, ☒ Frühere Mitarbeiter, ☐ Bewerber, ☐ Klienten, ☐ Interessenten, ☐ Dienstleister, ☒ Berater, ☒ Kontaktpersonen, ☐ Pressevertreter

Sonstige: Endkunden

## Anlage 2: Technisch-organisatorische Maßnahmen gemäß Art. 32 DS-GVO

### 1. Zugangskontrollen

Diese sollen gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt ist.

a. Technische Maßnahmen
    i. Manuelle Schließsysteme

b. Organisatorische Maßnahmen
    i. Videoüberwachung der Haupteingänge

### 2. Datenträgerkontrolle

Diese soll das unbefugte Lesen, Kopieren, Verändern und/oder Löschen von Datenträgern verhindern.

a. Technische Maßnahmen
    i. EDV-Zugang nur mit Benutzername und Passwort
    ii. Einsatz von Aktenvernichtern (Sicherheitsklasse 4 nach DIN 66399)
    iii. Ordnungsgemäße Vernichtung von Datenträgern (USB-Sticks, Festplatten)
    iv. Löschung von Datenträgern vor Wiederbenutzung

b. Organisatorische Maßnahmen
    i. Funktionsgeleitete Einschränkung der Benutzerberechtigung
    ii. Systemadministrator mit Generalzugang

### 3. Speicherkontrolle

Diese Kontrolle soll die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindern.

a. Technische Maßnahmen
    i. EDV-Zugang nur mit Benutzername und Passwort

b. Organisatorische Maßnahmen
    i. Funktionsgeleitete Einschränkung der Benutzerberechtigung
    ii. Systemadministrator mit Generalzugang

**4. Benutzerkontrolle**

Diese Kontrolle soll die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindern.

a. Technische Maßnahmen
    i. EDV-Zugang nur mit Benutzername und Passwort
    ii. Einsatz einer Firewall
    iii. Einsatz eines Anti-Viren-Programms

b. Organisatorische Maßnahmen
    i. Verwaltung der Benutzerrechte durch Systemadministrator
    ii. Erstellen eines Berechtigungskonzepts (welche Beschäftigtengruppe darf auf welche Daten wie zugreifen)
    iii. Empfang zur Personenkontrolle

**5. Zugriffskontrolle**

Diese Kontrolle soll gewährleisten, dass nur berechtigte Personen das EDV-System nutzen können und nur in dem ihnen eingeräumten Umfang.

a. Technische Maßnahmen
    i. EDV-Zugang nur mit Benutzername und Passwort
    ii. Beschränkung der Zugriffsrechte
    iii. Protokollierung von Zugriffen auf EDV-System hinsichtlich Eingabe, Veränderung, Kopie oder Löschung

**6. Eingabekontrolle**

Diese Kontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben wurden und/oder darin verändert worden sind.

a. Technische Maßnahmen
    i. EDV-Zugang nur mit Benutzername und Passwort
    ii. Protokollierung der Eingabe, Änderung und Löschung von Daten
    iii. Sicherstellung, dass das Protokoll dem Backup unterliegt

b. Organisatorische Maßnahmen
    i. Übersicht, mit welcher Software welche Daten eingegeben, geändert und gelöscht werden können

ii. Schaffung einer individuellen Benutzerkennung zum Nachvollziehen der Eingabe, Änderung oder Löschung

iii. Sicherung und Verwahrung von physischen Unterlagen, von denen Daten in das EDV-System importiert wurden

**7. Wiederherstellbarkeit**

Es soll gewährleistet werden, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

a. Technische Maßnahmen

i. Einsatz einer Backup-Software

b. Organisatorische Maßnahmen

i. Backup- und Recoveryplan

ii. Laufende Backup-Erstellung

iii. Turnusmäßiges Testen des Recoveryplans

iv. Aufbewahrung der physischen Backup-Kopien an einem weiteren sicheren Ort außerhalb der Geschäftsräume

**8. Zuverlässigkeit**

Es soll gewährleistet werden, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

a. Technische Maßnahmen

i. Regelmäßige Updates des Betriebssystems und sonstiger Programme

ii. Sicherung der Datenbankkonsistenz durch Integritätsbedingungen und entsprechender Fehlermeldung, sofern eine der Integritätsbedingungen verletzt wird

b. Organisatorische Maßnahmen

i. Pflicht der Beschäftigten zur Meldung von Fehlfunktionen

**9. Datenintegrität**

Es soll gewährleistet werden, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktion des Systems beschädigt werden können.

a. Technische Maßnahmen

i. Regelmäßige Updates des Betriebssystems und sonstiger Programme

**10. Verfügbarkeitskontrolle**

Diese Kontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

a. Technische Maßnahmen
    i. Schutzsteckdosen im Serverraum und an den Arbeitsplätzen
    ii. Thermometer und Hygrometer im Serverraum
    iii. Feuer- und Rauchmelder in den Geschäftsräumen
    iv. Feuerlöscher im Serverraum
b. Organisatorische Maßnahmen
    i. Serverräume nicht unter Sanitärräumen geplant

**11. Trennbarkeit**

Die Trennbarkeit soll gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden.

a. Technische Maßnahmen
    i. Datenverarbeitung erfolgt physikalisch getrennt auf gesonderten Betriebssystemen und/oder Datenträgern
    ii. Trennung von Produktiv- und Testsystem
b. Organisatorische Maßnahmen
    i. Kennzeichnung der Datensätze mit einer Zweckbestimmung
    ii. Trennung der Mandate durch Softwareeinstellung
    iii. Erstellung eines Berechtigungskonzepts
    iv. Festlegung von Zugriffs- und Datenbankrechten