Vereinbarung zur Auftragsdaten-verarbeitung

gemäß §11 BDSG

Software, Beratung und Services für Außenwirtschaft und Logistik

AEB

Vereinbarung zur Auftragsdatenverarbeitung (gemäß §11 BDSG)

zwischen:
(bitte nachfolgend ergänzen)

– im folgenden „Auftraggeber“ genannt –

Firma

Straße

PLZ/Ort

und:

AEB Gesellschaft zur Entwicklung von Branchen-Software mbH

– im folgenden „Auftragnehmer“ oder „AEB“ genannt –

Sigmaringer Str. 109,
70567 Stuttgart

Inhaltsverzeichnis

1	Anwendungsbereich, Verantwortlichkeit	4
2	Einzelheiten des Datenverarbeitungsauftrags	4
3	Weisungen des Auftraggebers	5
4	Technische und organisatorische Maßnahmen	6
5	Datengeheimnis, Kontrolle, öffentliches Verfahrensverzeichnis	6
6	Verstöße gegen datenschutzrechtliche Vorschriften oder Vereinbarungen	7
7	Auskünfte	7
8	Datenträger, Rückgabe, Löschung	7
9	Kontrollrecht und Prüfung durch den Auftraggeber	8
10	Unterauftragnehmer	8
11	Gefährdung durch Maßnahmen Dritter	9
12	Anwendbares Recht, Gerichtsbarkeit	9
13	Schlussbestimmungen	10
14	Anlagen	11

1 Anwendungsbereich, Verantwortlichkeit

a) Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag (einschließlich Anlagen wie z. B. Leistungsbeschreibung) in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

b) Der Hauptvertrag ergibt sich aus Aufträgen zu Leistungen des Auftragnehmers. Die Leistungen umfassen
- Erteilung zur Nutzung von durch AEB angebotenen Software-Lösungen
- sowie zugehörige Services (wie z. B. Support, Hosting).

Diese Aufträge (Verträge) sind in **Anlage 2** gelistet. Die Liste kann einvernehmlich erweitert werden. Beide Parteien beachten mögliche Auswirkungen auf den vorliegenden Vertrag zur Auftragsdatenverarbeitung.

c) Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Vor Beginn der Datenverarbeitung und sodann regelmäßig wird sich der Auftraggeber von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen und dies dokumentieren.

d) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. 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 verantwortlich. Der Auftraggeber bleibt „verantwortliche Stelle“ im Sinne der §§ 11, 3 Abs. 7 BDSG. Die in § 11 BDSG genannten Pflichten des Auftragnehmers bleiben hiervon unberührt.

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

2 Einzelheiten des Datenverarbeitungsauftrags

a) Gegenstand und Dauer des Auftrags ergeben sich aus dem Hauptvertrag (inkl. Supportvereinbarungen und Produkt-Leistungsbeschreibung). Mit Beendigung des Hauptvertrags endet der Auftrag.

b) Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen ergeben sich ebenfalls aus dem Hauptvertrag bzw. Leistungsbeschreibung.

c) Gemäß §11 Absatz 2 BDSG werden folgende näheren Angaben aus Sicht Auftraggeber gemacht zu
- **Datenkategorien:** Personalstammdaten, Kontaktdaten, Benutzerdaten, Kundendaten/ Adressen; zuzüglich
  i) Im Zusammenhang mit Produkten aus Import/Fracht/WUP zusätzlich: Lieferantendaten/Adressen
  ii) Im Zusammenhang mit Compliance ggf erweitern um Adress-Arten der Sanktionslistenprüfung

2 Einzelheiten des Datenverarbeitungsauftrags

- **Kreis der Betroffenen:** Kunden, Beschäftigte i.S. §3 Absatz 11 BDSG; zuzüglich
  - i) Im Zusammenhang mit Produkten aus Import/Fracht/WUP zusätzlich: Lieferanten
  - ii) Im Zusammenhang mit Compliance ggf erweitern um Betroffene aus Adressen der Sanktionslistenprüfung

d) Die Anwendungen beinhalten – sofern vom Auftraggeber nicht abweichend so gepflegt – keine besondere Arten personenbezogener Daten gemäß §3 BDSG.

e) Der Auftragnehmer erbringt die Leistung innerhalb des nachfolgend beschriebenen Raumes:

- EU / EWR
- Länder, die von der EU-Kommission als solche eingestuft sind, über ein angemessenes Datenschutz-Niveau zu verfügen.

Die Erbringung aus weiteren Ländern ist möglich, sofern einvernehmlich und nach Zustimmung des Auftraggebers sowie unter Beachtung der geltenden Gesetzgebung (etwa Art. 3, 44 ff. DS-GVO) entsprechende Sicherheiten hergestellt worden sind.

3 Weisungen des Auftraggebers

a) Der Auftragnehmer darf Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten und/oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang (Erhebung, Verarbeitung und/oder Nutzung) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung).

b) Der Auftraggeber kann durch Einzelweisungen die Berichtigung, Löschung und Sperrung von Daten verlangen.

c) Einzelweisungen des Auftraggebers, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind vom Auftragnehmer erst nach Einigung über deren Vergütung auszuführen, andernfalls gelten die jeweils gültigen Stundensätze des Auftragnehmers. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die durch eine hiermit verzögerte Ausführung dieser Einzelweisungen entstehen.

4 Technische und organisatorische Maßnahmen

a) Der Auftragnehmer trifft die gemäß § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen und gestaltet die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Schutzes personenbezogener Daten gerecht wird. Dies beinhaltet insbesondere

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- dafür zu sorgen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- dafür zu sorgen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- dafür zu sorgen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- dafür zu sorgen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- dafür zu sorgen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- dafür zu sorgen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

b) Die technischen und organisatorischen Maßnahmen sind in **Anlage 1** (Datensicherheit bei der AEB) enthalten. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses entsprechend einer technischen und organisatorischen Weiterentwicklung im Bereich des Auftragnehmers fortgeschrieben werden.

5 Datengeheimnis, Kontrolle, öffentliches Verfahrensverzeichnis

a) Die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter des Auftragnehmers sind gemäß § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen.

b) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Sein Kontakt: datenschutzbeauftragter@aeb.com. Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Landesbeauftragte Baden-Württemberg.

c) Soweit der Auftraggeber zur Führung eines öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gemäß § 4g Abs.2 S.2 BDSG verpflichtet ist, stellt der Auftragnehmer dem Auftraggeber die erforderlichen Informationen zur Verfügung, soweit eine Dienstleistung des Auftragnehmers gemäß diesem Auftrag berührt ist.

6 Verstöße gegen datenschutzrechtliche Vorschriften oder Vereinbarungen

Der Auftragnehmer wird Verstöße gegen datenschutzrechtliche Vorschriften oder vertragliche Regelungen durch ihn, eingesetzte Mitarbeiter oder sonstige Dritte dem Auftraggeber unverzüglich nach Kenntniserlangung mitteilen.

7 Auskünfte

Ist der Auftraggeber datenschutzrechtlich gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten; mit folgender Regelung: Aufwände, die dem Auftragnehmer in Wahrnehmung seiner Mitwirkung bei Auskünften entstehen, werden ihm durch den Auftraggeber mit einem Stundensatz von 100 EUR vergütet. Es ist dabei darauf zu achten, dass ein üblicher, vertrags- und vorgangstypisch zu erwartender Rahmen nicht überschritten wird. Bei Anzeichen eines Überschreitens ist die Vergütung gesondert und einvernehmlich zu vereinbaren.
Dem Auftraggeber ist bekannt, dass die Unterstützung (insbesondere Art, Umfang und Zeitraum der Unterstützung) vor allem davon abhängt, dass die Sicherheit von personen- und unternehmensbezogenen Daten anderer Kunden des Auftragnehmers nicht beeinträchtigt werden darf.

8 Datenträger, Rückgabe, Löschung

a) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Unbefugten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelweisung durch den Auftraggeber; hierfür entstehende Kosten übernimmt der Auftraggeber.

b) Der Auftragnehmer hat nach Ende des Hauptvertrags auf Anforderung des Auftraggebers Daten und Datenträger herauszugeben bzw. zu löschen oder zu sperren gemäß BDSG, soweit nicht gesetzliche Aufbewahrungsfristen des Auftragnehmers entgegenstehen. Die Einhaltung des Trennungsgebots nach BDSG ist hiervon nicht berührt. Die Anforderung soll vom Auftraggeber schriftlich innerhalb eines Monats nach Vertragsende erklärt werden. Kosten, die durch die Herausgabe, Löschung oder Sperrung beim Auftragnehmer entstehen, trägt der Auftraggeber.

c) Hinsichtlich der Original- und Ergebnisdateien im Zusammenhang mit Compliance ist AEB berechtigt, diese Daten nach Ablauf von 31 Tagen (gezählt ab Durchführung der Prüfung) zu löschen.

9 Kontrollrecht und Prüfung durch den Auftraggeber

a) Der Auftraggeber kann selbst oder durch beauftragte Dritte nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG prüfen. Aufwände, die dem Auftragnehmer in Wahrnehmung seiner Mitwirkung bei Kontrollen entstehen, werden ihm durch den Auftraggeber ab Übersteigen eines üblichen Aufwands (bis zu 4 Personenstunden pro Jahr) mit einem Stundensatz von 100 EUR vergütet. Es ist dabei darauf zu achten, dass ein üblicher, vertrags- und vorgangstypisch zu erwartender Rahmen nicht überschritten wird. Bei Anzeichen eines Überschreitens ist die Vergütung gesondert und einvernehmlich zu vereinbaren.

b) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

c) Das Kontrollrecht erstreckt sich nicht auf Bereiche, die Betriebs- und Geschäftsgeheimnisse des Auftragnehmers berühren, es sei denn, personenbezogene Daten des Auftraggebers, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen, sind von diesen Bereichen betroffen.

d) Die im Rahmen der Ausübung des Kontrollrechts bei Vor-Ort-Audits erhobenen Befunde und Ergebnisse sind schriftlich abzufassen und dem Auftragnehmer kostenfrei zur Verfügung zu stellen.

e) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

10 Unterauftragnehmer

a) Dem Auftraggeber ist bekannt, dass AEB als IT-Provider Leistungen für eine Vielzahl von Kunden erbringt. Entsprechend werden auch Unterbeauftragungen in der Regel Kunden-anonym erteilt

b) Die vertraglich vereinbarten Leistungen werden zum Zeitpunkt des Vertragsschlusses unter Einschaltung folgender Unterauftragnehmer durchgeführt:

Unterauftragnehmer	Funktion	Standort
AFI Solutions GmbH	Wartung und Support zu Software für Middleware (Kommunikationssoftware)	Stuttgart
Trivadis GmbH	Datenbank-Administration und -Support	Stuttgart
Hewlett Packard GmbH	Hardware-Lieferant	Böblingen

c) Der Auftragnehmer kann ohne gesonderte schriftliche Zustimmung zur Vertragsdurchführung konzernangehörige Unternehmen sowie andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung frühzeitig (i.d.R. wenigstens 6 Wochen vor Beginn der Datenverarbeitung) mitteilt.

d) Die vertraglichen Vereinbarungen mit den Unterauftragnehmern werden so gestaltet, dass sie den vereinbarten Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Parteien entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend Ziffer 9 einzuräumen. Der Auftraggeber ist berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten im Zusammenhang mit der Auftragsdatenverarbeitung stehenden vertraglichen Vereinbarungen.

10 Unterauftragnehmer

e) Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

f) Sofern nach Ablauf einer Frist von 4 Wochen ab Eingang der Information über Hinzunahme oder Änderung in einer Unterbeauftragung kein Einspruch seitens des Auftraggebers eingeht, gilt die Unterbeauftragung gemäß der allgemeinen schriftlichen Genehmigung als bestätigt.

g) Der Auftraggeber wird darauf achten, eine Zustimmung nicht unbillig zu verweigern und einen Einspruch nicht ohne wichtigen, für den Auftragnehmer nachvollziehbaren Grund zu erheben.

11 Gefährdung durch Maßnahmen Dritter

Werden die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer wird ferner alle ihm in diesem Zusammenhang bekannten relevanten Dritte unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

12 Anwendbares Recht, Gerichtsbarkeit

a) Diese Vereinbarung unterliegt deutschem Recht. Die Geltung des UN-Übereinkommens über Verträge über den internationalen Warenkauf (CISG) ist ausgeschlossen.

b) Für alle Streitigkeiten, die sich im Zusammenhang mit diesem Vertrag, Vertragserweiterungen oder -ergänzungen oder über seine Gültigkeit ergeben, die die Parteien nicht untereinander bereinigen können, kann nach Wahl der AEB ein Schlichtungsverfahren eingeleitet und/oder eine Entscheidung der Streitigkeit durch ein Schiedsgericht unter dem Ausschluss des ordentlichen Rechtsweges bzw. die Entscheidung der Streitigkeit durch die ordentliche Gerichtsbarkeit herbeigeführt werden.

c) AEB ist verpflichtet, als künftige Beklagte oder in sonstiger Weise passiv Beteiligte eines gerichtlichen Verfahrens ihr Wahlrecht bereits vorprozessual innerhalb von zwei Wochen nach Zugang einer schriftlichen Aufforderung des Vertragspartners auszuüben. Geht dem Vertragspartner innerhalb dieser Frist keine schriftliche Wahl der

12 Anwendbares Recht, Gerichtsbarkeit

AEB zu, kann AEB die Durchführung eines Schlichtungsverfahrens nicht mehr verlangen und die Einrede der Schiedsgerichtsbarkeit nicht erheben.

d) Wählt AEB das Schlichtungsverfahren, wird die Schlichtungsstelle der Deutschen Gesellschaft für Recht und Informatik (www.dgri.de) angerufen, um den Streit nach deren Schlichtungsordnung in der zum Zeitpunkt der Einleitung eines Schlichtungsverfahrens gültigen Fassung ganz oder teilweise, vorläufig oder endgültig zu bereinigen. Die Verjährung für alle Ansprüche aus dem schlichtungsgegenständlichen Lebenssachverhalt ist ab dem Schlichtungsantrag bis zum Ende des Schlichtungsverfahrens gehemmt. § 203 BGB gilt entsprechend.

e) Wählt AEB die Entscheidung durch ein Schiedsgericht, wird die Streitigkeit nach der Schiedsgerichtsordnung der Industrie- und Handelskammer Region Stuttgart unter Ausschluss des ordentlichen Rechtsweges endgültig entschieden. Der Ort des schiedsrichterlichen Verfahrens ist Stuttgart. Das Schiedsgericht besteht aus einem Einzelschiedsrichter. Das anwendbare materielle Recht ist deutsches Recht. Die Sprache des schiedsrichterlichen Verfahrens ist deutsch.

f) Wählt AEB die Entscheidung durch die ordentliche Gerichtsbarkeit, ist der Gerichtsstand am Sitz von AEB; AEB ist aber auch berechtigt, Ansprüche am Sitz des Vertragspartners geltend zu machen.

13 Schlussbestimmungen

Ergänzungen und sonstige Änderungen dieser Anlage bedürfen der Schriftform (§ 11 Abs.2 BDSG).

14 Anlagen

Anlage 1: Aufstellung der technischen und organisatorischen Maßnahmen; als beigefügtes Dokument zum aktuellen Stand (30.06.2016) mit Titel: „Datensicherheit bei der AEB Gesellschaft zur Entwicklung von Branchen-Software mbH“.

Anlage 2: Auflistung der Verträge, die eine Grundlage für den Vertrag zur Auftragsdatenverarbeitung darstellen. Gemeinsam hier als Hauptvertrag geltend.

Auftraggeber	**Auftragnehmer**
Ort	Ort
Datum	Datum
Name / Funktion	Name / Funktion
Unterschrift	Unterschrift

Datensicherheit bei der AEB

Gesellschaft zur Entwicklung von Branchen-Software mbH

(Technische und Organisatorische Maßnahmen / Controls)

Anlage 1, Stand: 30.06.2016

Software, Beratung und Services für Außenwirtschaft und Logistik

AEB

Inhaltsverzeichnis Anlage 1

A	**Grundsätzliches zum Dokument**	**14**
1.	Verwendungszweck Datenschutz	14
2.	Verwendungszweck SOX Compliance	14
B	**Beschreibung der generellen Kontrolle**	**14**
1.	Applikationsablaufkontrolle	14
2.	Allgemeine organisatorische Kontrolle (Managementsysteme)	15
3.	Technische und organisatorische Maßnahmen	15
C	**Beschreibung der Applikationskontrolle**	**17**
1.	Qualitätssicherung	17
2.	Qualitätssicherung durch definierte Prozesse	17
3.	Qualitätssicherung durch externe Prüfer	17

A Grundsätzliches zum Dokument

Dieses Dokument führt alle Sicherheits-Kontrollsysteme der Services des Rechenzentrums der AEB Gesellschaft zur Entwicklung von Branchen-Software mbH auf.
Die Maßnahmen können sowohl technischer als auch organisatorischer Natur sein. Sie müssen auf dem Stand der Technik sein und auch den Faktor Mensch einschließen.
AEB ist berechtigt, die erforderlichen Maßnahmen anzupassen, sofern das bisher erreichte Sicherheitsniveau nicht unterschritten wird. Die dargestellten Maßnahmen sind kundenanonym übergreifend ausgelegt.
Dieses Dokument ist mit Angabe des Datums (Stand) versioniert.

1. Verwendungszweck Datenschutz

Nach geltenden Gesetzen (z. B. Bundesdatenschutzgesetz mit §9 BDSG und Anlage, künftig die EU-Datenschutz-Grundverordnung) sind geeignete technische und organisatorische Maßnahmen zu wählen, die dem erforderlichen Schutzbedarf der (personenbezogenen) Daten entsprechend den gesetzlichen Anforderungen genügen. Erforderlich sind Maßnahmen nur, soweit ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

2. Verwendungszweck SOX Compliance

Aufgrund der Anforderungen an ServiceProvider, die vor allem im Abschnitt 404 des Sarbanes-Oxley Acts (SOX) formuliert sind, sollen ausgelagerte Compliance-relevante Aufgaben eines Unternehmens, das dem SOX unterliegt, auch geprüft werden.
Um diese Überprüfung zu vereinfachen, gibt es die Möglichkeit, einen Bericht (Zertifizierung) über die ausgelagerten Services erstellen zu lassen. In diesem Report beschreibt der Service Provider selber sein internes Kontrollsystem (Datenschutz, Datensicherheit, Zugriffssicherheit, Datenintegrität etc.). Dieses Kontrollsystem muss angemessen ausgestaltet sein, um die angegebenen Ziele zu erreichen. Und es muss vollständig implementiert sein. Die Relevanz kann von einem externen Prüfer bescheinigt werden.
Weitere Hinweise dazu:

- SSAE16 (Statement on Standards for Attestation Engagements No. 16) mit Bezug zu Standard ISAE 3402 (International Standard on Assurance Engagements No. 3402)
- In Deutschland gibt es auch den Prüfungsstandard PS 951 des IDW (Institut der Wirtschaftsprüfer in Deutschland e.V.), der sich auf den Standard ISAE 3402 bezieht.
- Frühere Grundlage: SAS 70 (Report Type 2)

B Beschreibung der generellen Kontrolle

1. Applikationsablaufkontrolle

Sorge zu tragen, dass Applikationen richtig implementiert sind und die richtige Datenverarbeitung durch die Applikationen erfolgt.

- Sowohl die Services als auch die zugehörigen Techniken und Prozesse werden von der Koordinierenden Stelle (KoSt) ATLAS bei der Oberfinanzdirektion Karlsruhe geprüft und nur bei vollständiger Abbildung der Anforderungen zertifiziert.
- Prüf- und Zertifizierungsprotokolle liegen auch der KoSt ATLAS vor.

B Beschreibung der generellen Kontrolle

2. Allgemeine organisatorische Kontrolle (Managementsysteme)

2.1 Datenschutz

Der betriebliche Datenschutzbeauftragte prüft und kontrolliert die Einhaltung der Vorschriften des BDSG. Der Datenschutzbeauftragte hält ein Datenschutzkonzept verfügbar. Einige der nachfolgend geschilderten Kontrollen sind verpflichtend gemäß §9 BDSG (technische und organisatorische Maßnahmen).

Eine begrenzte Auswahl aus den IT-Teams vergibt Zugangsberechtigungen mit Vier-Augen-Prinzip. Die Berechtigungen werden regelmäßig ereignis- und zeitgesteuert kontrolliert; insbesondere mit Blick auf den Betrieb des Rechenzentrums. Die obige Auswahl kann Einspruch erheben und ihr Veto einlegen.

2.2 Sicherheitskontrolle, Risikomanagement

Der Betrieb des ISMS (Information Security Management System in Verbindung mit dem Zertifikat zur ISO 27001) stellt das IT-Security Management als kontinuierlichen prozessorientierten PDCA-Kreislauf sicher. Dieser Prozess basierend auf assets (Informationen, Werten) schließt Schutzbedarfsermittlung und detaillierte Risikobetrachtungen (Risikobewertung und -behandlung) ein. Die wichtigsten und relevanten Sicherheitskriterien sind

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Das ISMS enthält Kontrollen u. a. in Form von internen und externen Audits sowie regelmäßige Managementbewertungen. Eine weitere Ebene ist die Sicherstellung eines hohen Sicherheitsbewußtseins (security awareness) mit Hilfe diverser Maßnahmen zur Aus- und Weiterbildung der Beschäftigten.

Für eine umfassende Darstellung verweisen wir auf unsere Informationssicherheitsleitlinie (als Teil der Leitlinie Integriertes Managementsystem) in http://service.aeb.com/open/leitlinien-und-zertifikate.

3. Technische und organisatorische Maßnahmen

3.1 Eingabekontrolle

Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Alle Produkte, die personenbezogene Daten verarbeiten, protokollieren sämtliche Eingaben, Änderungen, Löschungen. Diese Protokollierung stellt sicher, dass nachträglich festgestellt werden kann, ob und wenn von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.
- Personalisierte Benutzerkonten auch in den Fachanwendungen.
- Trennung von System- und Anwendungsprotokollen, dadurch ist eine Manipulation der Anwendungsprotokolle auf Systemebene ausgeschlossen.

3.2 Auftragskontrolle

Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Regelung der Weisungen im Hauptleistungs- und Auftragsdatenverarbeitungsvertrag
- Benutzer- und Rechteverwaltung auf Anwendungsebene durch den Auftraggeber.
- Übermittlung/Erfassung der Daten durch den Auftraggeber. Er entscheidet, wann welche Daten übermittelt werden.
- Zugriff auf diese Daten haben nur Rollen mit entsprechender Zugriffsbefugnis
- Automatisierte Verarbeitung der Daten durch zertifizierte Software (Verfahren ATLAS, Compliance). Dadurch wird sichergestellt, dass die Daten gem. beauftragten Verfahren verarbeitet werden.
- Einsatz von Standardverträgen gemäß §11 BDSG für Verhältnisse mit Kunden und Dienstleistern
- Einbindung von Subunternehmen mit entsprechenden Verträgen zu Vertraulichkeit, Auftragsdatenverarbeitung, Systemzugang.

B Beschreibung der generellen Kontrolle

3.3 Trennungskontrolle

Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von:
  - Mitarbeiterdaten
  - Kundenkontaktdaten
  - Kundentestdaten (Projektarbeit, Kundenentwicklungen)
  - Fernwartungszugangsdaten
  - Kundendaten im AEB-Rechenzentrum
- Systemebene:
  - Kundendaten im Rechenzentrum werden von Daten der AEB (u. a. auch zu CRM-System) streng getrennt und in verschiedenen Systemen (Datenbanken etc.) verwaltet.
- Unterschiedliche Anwendungen:
  - Für Kundendaten und Mitarbeiterdaten werden unterschiedliche Anwendungen eingesetzt.
- Berechtigungen innerhalb der Anwendung:
  - Kundenkontaktdaten sind streng von Fernwartungszugangsdaten getrennt.

3.4 Zutrittskontrolle

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehren.

- Mehrstufige technische Schließsysteme, teilweise mit Ausrüstung zur Alarmierung.
- Sicherung des Gebäudes und Identitätskontrolle aller Anwesenden außerhalb der Geschäftszeiten durch einen Wachdienst.
- Regelung zur Zutrittsberechtigung für Nicht-Angestellte.
- Zentrale Aufbewahrung zur Vergabe von elektronischen Codeschlüsseln (Tokens), Protokollierung der Aus- und Rückgabe.
- Server und Fernwartungsrouter sind durch Zutrittskontrolle (Codeschlössser, Codeschlüssel) zum Serverraum geschützt.
- Fernwartungssysteme sind gesichert durch:
  - Zugriff auf Fernwartungsdaten nur für Berechtigte.
  - Systeme für Fernwartungszugänge zu Kunden stehen in einer abgeschotteten Netzwerkumgebung.

3.5 Zugangskontrolle

Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Arbeitsplatzrechner sind gesichert durch:
  - Anmeldung nur durch zentral gesteuertes Identity Management.
  - Verpflichtung der Mitarbeiter zur Sperrung des Arbeitsplatzrechners.
  - Automatische Sperrung der Arbeitsplatzrechner nach höchstens 15 Minuten.
  - Zentrale Kennwortrichtline auch für Administrationszugänge (regelmäßiger Zwang zur Änderung der Kennwörter, Mindestanforderung an Kennwortlänge und Komplexität).

3.6 Zugriffskontrolle

Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Zentrale Berechtigungsverwaltung, getrennt für System- und Anwendungszugang.
- Anwender können Berechtigungen nicht selbständig ändern.
- Anwender können nicht ohne Freigabe durch Vorgesetzten eine Änderung beantragen.
- Grundsätzlich keine externen Zugänge außer VPN- bzw. SSH gesicherte Verbindungen.
- Sicherheitsprüfungen der externen Zugänge durch darauf spezialisierte Firmen.
- Regelung bei Aufgabenwechsel innerhalb Unternehmen.

3.7 Weitergabekontrolle

Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

B Beschreibung der generellen Kontrolle

- Der unternehmensweite Security Guide verbietet grundsätzlich den Versand von unverschlüsselten Daten.
- Alle Download/Uploadverbindungen via Internet sind gesichert durch entweder SSL, SSH oder VPN.
- Alle Niederlassungen bzw. mobilen Systeme verwenden ausschließlich VPN oder SSH gesicherte Verbindungen, die der Hoheit der AEB unterliegen.
- Es findet keine lokale Speicherung personenbezogener Daten statt, alle Daten werden zentral in Stuttgart gehalten.
- Externe Verbindungen sind nur über freigegebene Anwendungen möglich.
- Externe Verbindungen sind nur über freigegebene Services möglich.
- Alle DFÜ-Verbindungen werden protokolliert soweit technisch machbar.
- Regelung zur Entsorgung von Abfällen mit vertraulichen Inhalten im Einklang mit relevanten DIN-Vorschriften (zu Schutzklasse und Sicherheitsstufen)

3.8 Verfügbarkeitskontrolle

Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Redundante Systeme:
  - Datenbank: Cluster (bei Bedarf)
  - Fileserver: Cluster
  - SAN/Storage: redundante Komponenten
- Unterbrechungsfreie Stromversorgung
- Brandmelde- bzw. Brandlöschanlagen
- Bandsicherung:
  - Tägliche Bandsicherung
  - Auslagerung der Daten in gesonderten Brandabschnitt/gesondertes Gebäude
  - Zuzüglich untertags regelmäßige Sicherung der Nutzdaten auf Basis Datenbank-Tools
- Führen eines Notfallkonzepts (Business Continuity Management) zur Notfall-Prävention und -Bewältigung

C Beschreibung der Applikationskontrolle

1. Qualitätssicherung

Qualität steht in allen Bereichen der AEB im Vordergrund. Ihr wird eine besondere Stellung eingeräumt. Aufgaben- und Prozessverantwortliche definieren, optimieren und prüfen die Prozesse der Applikationsentwicklung, aber auch der Wartung und des Services anhand des PDCA-Kreislaufs.

Im Bereich der Applikationen werden dabei nicht nur Funktions- sondern auch Usability-Tests durchgeführt. Jede Neuerung wird dabei mehrfach geprüft und abgenommen.

Aktualität fachlicher Anforderungen wird ständig verfolgt und umgesetzt. Im engen Kundenkontakt wird Wartung und Service bewertet und optimiert. Die Arbeitsweise ist service- und prozessorientiert.

2. Qualitätssicherung durch definierte Prozesse

Alle Schritte der Neuentwicklung sowie die Wartung der Applikationen durchlaufen definierte und kommunizierte Prozesse (Prinzip der Transparenz). Alle Applikationsentwicklungs- und Wartungsaufgaben werden als Projekte mit definiertem Projektablauf (manifestiert in Muster-Projekten) und einem beschriebenen Prozess realisiert. Darin integriert ist ein umfassendes Rollenkonzept mit diversen Stufen der Freigaben unter Nutzung des Vier-Augen-Prinzips. Zur Sicherstellung der Compliance sind außerdem Sicherheits-Checks vorgesehen.

C Beschreibung der Applikationskontrolle

3. Qualitätssicherung durch externe Prüfer

Applikationen werden – wo erforderlich – auch durch externe Prüfer geprüft und zertifiziert.
Dies geschieht u. a. in Anlehnung an IDW-Prüfungsstandards und Stellungnahmen wie IDW PS 330 („Abschlussprüfung bei Einsatz von Informationstechnologie“) oder IDW RS FAIT 1 („Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie“).

Auflistung der Verträge

Anlage 2

Vertragsliste

Nachfolgend werden die Verträge gelistet, die eine Grundlage für den Vertrag zur Auftragsdatenverarbeitung zwischen Auftraggeber und Auftragnehmer darstellen:

- ...
- ...
- ...