Beispiel für einen Einsatz des Muster-ADV-Vertrages

Einführung

Am Beispiel eines EVB-IT-Vertrages für die Dienstleistung „Wartung/Fernwartung“ wird dargestellt, wie anhand des Muster-ADV-Vertrages durch individuelle Anpassung ein ADV-Vertrag aussehen könnte.

Abgrenzung

Dies ist nur ein Beispiel und ist nicht dazu geeignet, 1:1 in der Praxis eingesetzt zu werden.

Beschreibung des Beispiel-Szenarios

Das Krankenhaus „Fröhliche Himmelspforte“ setzt das Krankenhausinformationssystem (KIS) „health club“ des Herstellers „Health Software Shop“ (HSS) ein. Die Anschaffung erfolgte mittels eines EVB-IT Vertrages. Auch die Software wurde vertraglich über einen entsprechenden Vertrag (EVB–IT Pflege S) vereinbart.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Vertrag über die Pflege von Standardsoftware

Vertragsnummer/Kennung Auftraggeber 2014-0815

Vertragsnummer/Kennung Auftragnehmer 2014-4711

EVB-IT Pflegevertrag S

Zwischen dem Krankenhaus „Fröhliche Himmelspforte“

- im Folgenden „Auftraggeber“ genannt -

und

dem Hersteller „Health Software Shop“ (HSS)

- im Folgenden „Auftragnehmer“ genannt -

wird folgender Vertrag geschlossen:

1 Vertragsgegenstand und Vergütung

1.1 Vertragsgegenstand ist die Pflege von Standardsoftware* gemäß Nummer 3.

1.2 Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung.

1.3 Die Leistungen des Auftragnehmers werden

☒ gegen eine monatliche Pauschale gemäß Nummer 6.1.1 in Höhe von 666,66 €

☐ gegen eine abweichende monatliche Pauschale gemäß Nummer 6.1.2 für die dort vereinbarten Zeiträume

☐ gegen eine einmalige Pauschale gemäß Nummer 6.1.1 in Höhe von _____

☐ gegen eine Vergütung nach Aufwand gemäß Nummer 6.2.1

zuzüglich der zum Zeitpunkt der Leistungserbringung gültigen Umsatzsteuer vergütet.

2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- Dieser Vertrag (Seite 1 bis xxx) einschließlich der Anlage(n) Nr. _____
- Ergänzende Vertragsbedingungen für die Pflege von Standardsoftware* (EVB-IT Pflege S) in der bei Vertragsschluss geltenden Fassung einschließlich der Muster 1 und 2
- Verdingungsordnung für Leistungen — ausgenommen Bauleistungen — Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung.
- Allgemeine Einkaufsbedingungen des Auftraggebers
- Auftragsdatenverarbeitungsvertrag vom _____

EVB-IT Pflege S und VOL/B liegen beim Auftraggeber zur Einsichtnahme bereit, desgleichen die allgemeinen Einkaufsbedingungen und das für Wartung gültige Service Level Agreement.

2.2 Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

3 Art und Umfang der Pflegeleistungen

Der Auftragnehmer erbringt für den Auftraggeber die folgenden Pflegeleistungen:

3.1 Pflegeleistungen zur Mängelbehebung

3.1.1 ☒ Basispflegeleistung

☒ Bereitstellung verfügbarer Umgehungen*, Patches* und Updates* .

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

☐ Auf Anforderung des Auftraggebers innerhalb der Reaktionszeit* .

☒ Unverzüglich sobald verfügbar.

Art der Lieferung:

☒ Postalischer Versand; Datenträger: _____

☒ Elektronische Zustellung; Adresse: _____

☒ Bereitstellung im Internet zum Download; Adresse: _____

Zusätzliche Unterstützungsleistung für die Basispflegeleistung

☒ Unterstützung des Auftraggebers bei der Umsetzung einer Umgehung* bzw. der Installation von Patches* und Updates* .

Art der Leistungserbringung der zusätzlichen Unterstützungsleistung:

☒ Die Leistung wird als Teleservice* gemäß Anlage Nr. (Teleservicevereinbarung)

erbracht.

☐ Die Leistung wird als Vor-Ort-Service* erbracht. Adresse: (ggf. Rechner)

☐ Sonstige Art der Leistungserbringung gemäß Anlage Nr. .

3.1.2 ☐ Additive Pflegeleistungen (Mängelbehebung) gegen Vergütung nach Aufwand

3.2 Lieferung von Upgrades*, Releases*/Versionen*

3.2.1 ☒ Upgrade*-Service

☒ Bereitstellung verfügbarer Upgrades* ohne Verpflichtung bezüglich Häufigkeit und Umfang.

☐ Auf Anforderung des Auftraggebers innerhalb der Reaktionszeit* .

☒ Unverzüglich sobald verfügbar.

Art der Lieferung:

☒ Postalischer Versand; Datenträger: _____

☒ Elektronische Zustellung; Adresse: _____

☒ Bereitstellung im Internet zum Download; Adresse: _____

3.2.2 ☒ Release*-/Versions*-Service

☐ Bereitstellung verfügbarer Releases*/Versionen* ohne Verpflichtung bezüglich Häufigkeit und Umfang.

☐ Auf Anforderung des Auftraggebers innerhalb der Reaktionszeit* .

☒ Unverzüglich sobald verfügbar.

Art der Lieferung:

☒ Postalischer Versand; Datenträger: _____

☒ Elektronische Zustellung; Adresse: _____

☒ Bereitstellung im Internet zum Download; Adresse: _____

3.3 Umsetzungs- und Installationsleistungen

☒ Umsetzung von Umgehungen* und Installation* von Patches* und Updates* gemäß der in Nummer 3.1.1 vereinbarten Basispflegeleistung.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

☒ Installation von Upgrades*, Releases*/Versionen* gemäß Nummer 3.2.

Art der Installation:

☒ Die Leistung wird als Teleservice* gemäß Anlage Nr. (Teleservicevereinbarung) erbracht.

☐ Die Leistung wird als Vor-Ort-Service* erbracht; Adresse: (ggf. Rechner)

☐ Sonstige Art der Leistungserbringung gemäß Anlage Nr. .

3.4 Weitere Pflegeleistungen

3.4.1 ☒ Informationsservice

Unverzügliche Bereitstellung verfügbarer Informationen über bekannt gemachte Programmkorrekturen* durch:

☒ Postalischer Versand; Datenträger: _____

☒ Elektronische Zustellung; Adresse: _____

☒ Bereitstellung im Internet zum Download; Adresse: _____

3.4.2 ☒ Hotline-Service gemäß Anlage Nr. während der vereinbarten Servicezeiten*.

3.4.3 ☐ Sonstige Pflegeleistungen gemäß Anlage Nr. .

4 Ergänzende Beschreibung der Pflegeleistung

Die Beschreibung der Pflegeleistung ergibt sich ergänzend aus

☒ folgenden Teilen des Angebotes des Auftragnehmers vom 02.02.2014

☒ folgenden Teilen der Leistungsbeschreibung des Auftraggebers vom …

☐ folgenden weiteren Dokumenten

Es gelten die Dokumente in

☒ obiger Reihenfolge

☐ folgender Reihenfolge:

5 Nutzungsrechte* des Auftraggebers und Bearbeitungsrechte durch Dritte*

☒ Die Standardsoftware* gemäß Nr. 6.1.1 lfd. Nr. darf zeitlich und mengenmäßig unbeschränkt genutzt werden.

☐ Die Standardsoftware* gemäß Nr. 6.2.1 lfd. Nr. darf bis zu -fach genutzt werden.

☐ Sonstige Angaben zum Nutzungsrecht* des Auftraggebers und/oder Bearbeitungsrechte durch Dritte* gemäß Anlage Nr. .

☒ Das Nutzungsrecht an der Standardsoftware* gemäß Nr. 6.1.1 lfd. Nr. gilt für Tochter- und Beteiligungsgesellschaften des Auftraggebers und seinen Rechtsnachfolgern.

6 Standardsoftware* und Vergütung

6.1 Pflege gegen pauschale Vergütung

6.1.1 Produkte, Leistungsdauer, Pauschale

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Lfd. Nr.	Produktbezeichnung und -beschreibung Release-/Versions-Nr. Produkt-Nr.	Anzahl/ Lizenz-art	Pflege-leistung gemäß Nummer 3.__	MVD in Mona-ten	Leistungsdauer Beginn	Leistungsdauer Ende	Monatliche Pauschale netto Einzel-preis	Monatliche Pauschale netto Summe Preis	Einmalige Pauschale netto Einzel-preis	Einmalige Pauschale netto Summe Preis
1	2	3	4	5	6	7	8	9	10	11
							Gesamtpreis (netto)	monatlich		einmalig

MVD = Mindestvertragsdauer*, gerechnet ab vereinbartem Beginn der Leistungsdauer.

6.1.2 Abweichende monatliche Pauschale ab Beginn der Leistungsdauer

Lfd. Nr. gemäß Nummer 6.1.1, Spalte 1	Ende des Zeitraumes der abweichenden Vergütung	von Nummer 6.1.1 abweichende monatliche Pauschale netto Einzelpreis	Summe Preis	Abweichend vom monatlichen Gesamtpreis gemäß Nummer 6.1.1 ergeben sich für folgende Zeiträume nachstehende monatliche Gesamtpreise von	bis	**Gesamtpreis (netto)**
1	2	3	4	5	6	7

Zwischen folgenden Produkten aus Nummer 6.1.1 besteht ein funktionaler Zusammenhang (Ziffer 7.3 Absatz 4 EVB-IT Pflege S):

6.1.3 Rechnungsstellung bei pauschaler Vergütung

Die Rechnungsstellung erfolgt

- ☐ monatlich (zahlbar bis zum 15. eines jeden Monats)
- ☐ quartalsweise (zahlbar bis zum 15. des zweiten Quartalmonats)
- ☒ jährlich (zahlbar bis zum 15. Januar)
- ☐ einmalig zum _____.
- ☐ _____.

6.1.4 Reaktionszeit*, Servicezeiten*

6.1.4.1 1 Reaktionszeit* (abweichend von Ziffer 1.7 EVB-IT Pflege S)

☐ Es wird folgende Reaktionszeit* vereinbart:

Die Pflegeleistungen beginnen, gerechnet vom Zugang der Störungsmeldung an, innerhalb von 4 Stunden während der vereinbarten Servicezeiten*.

☒ Andere Vereinbarungen zur Reaktionszeit* gemäß Anlage Nr.

Service Level Agreement.

6.1.4.2 Servicezeiten*

Es werden folgende Servicezeiten* vereinbart:

_____ bis _____ von _____ bis _____ Uhr.

_____ bis _____ von bis Uhr.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

_____ von _____ bis _____ Uhr.

Für Feiertage gilt ☐ Die o.a. Zeiten gelten nicht an Feiertagen am Erfüllungsort.

☐ _____

☒ Weitergehende Vereinbarungen zu den Reaktions*- und Servicezeiten* gemäß Anlage Nr. .

Service Level Agreement

6.2 Pflegeleistung gegen Vergütung nach Aufwand

6.2.1 Produkte, Leistungsdauer, Vergütung

Lfd. Nr.	Produktbezeichnung und -beschreibung Release-/Versions-Nr. Produkt-Nr.	Anzahl / Lizenz-art	Pflege-leistung gemäß Nummer 3.__	Leistungsdauer		Preis je Stunde netto gem. Nummer 6.2.2.1	Preis je Stunde netto gem. Nummer 6.2.2.2
				Beginn	Ende		
1	2	3	4	5	6	7	8

6.2.2 Zeiten der Leistungserbringung bei Vergütung nach Aufwand

Die Leistungen des Auftragnehmers werden erbracht

6.2.2.1 ☒ während der üblichen Geschäftszeiten des Auftragnehmers an Werktagen (außer an Samstagen)

_____ bis _____ von _____ bis _____ Uhr.

6.2.2.2 ☒ während sonstiger Zeiten

_____ bis _____ von _____ bis _____ Uhr.
an Sonn- und Feiertagen am Sitz des Auftragnehmers von bis Uhr.

6.2.3 Weitere Vergütungsregelungen

6.2.3.1 Reisezeiten

☒ Reisezeiten werden nicht gesondert vergütet.

☐ Reisezeiten werden vergütet gemäß Anlage Nr. .

6.2.3.2 Reisekosten* und Nebenkosten*

☒ Reisekosten* und Nebenkosten* werden nicht gesondert vergütet.

☐ Reisekosten und Nebenkosten* werden vergütet gemäß Anlage Nr. .

6.2.4 Reaktionszeit*, Servicezeiten*

6.2.4.1 1 Reaktionszeit* (abweichend von Ziffer 1.7 EVB-IT Pflege S)

☐ Es wird folgende Reaktionszeit* vereinbart:

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Die Pflegeleistungen beginnen, gerechnet vom Zugang der Störungsmeldung an, innerhalb von Stunden während der vereinbarten Servicezeiten*.

☒ Andere Vereinbarungen zur Reaktionszeit* gemäß Anlage Nr. .

Service Level Agreement

6.2.4.2 Servicezeiten*

Es werden folgende Servicezeiten* vereinbart

	bis	von	bis	Uhr.
Für Feiertage gilt	☐	Die o. a. Zeiten gelten nicht an Feiertagen am Erfüllungsort.		
	☐			

☒ Weitergehende Vereinbarungen zu den Reaktions*- und Servicezeiten* gemäß Anlage Nr. .

Service Level Agreement

6.2.5 Vorhaltepauschale

☒ Das Vorhalten von Personal und Material wird nicht gesondert vergütet.

☐ Das Vorhalten von Personal und Material wird in Form einer Pauschale zusätzlich vergütet gemäß Anlage Nr. .

7 Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt

0 auf die monatliche Pauschale vereinbart

0 gemäß Ziffer 6.3 EVB-IT Pflege S.

0 anderweitige Regelung gemäß Ziffer 6.3 EVB-IT Pflege S.

0 auf die Stundenverrechnungssätze nach Aufwand vereinbart

0 gemäß Ziffer 6.3 EVB-IT Pflege S.

0 anderweitige Regelung gemäß Ziffer 6.3 EVB-IT Pflege

8 Störungsmeldung

8.1 Adresse für Störungsmeldung

Die Störungsmeldung erfolgt auf einem Formular entsprechend Muster 1 zu EVB-IT Pflege S – Störungsmeldeformular – an:

Name/Firma: _____
Organisationseinheit/Abteilung: _____
☒ Postanschrift: _____
☒ Telefon: _____
☒ Fax: _____
☒ E-Mail: _____
☒ Web-Adresse: _____

8.2 Annahme der Störungsmeldung

Die Störungsmeldung wird während der in den Nummern 6.1.4.2 bzw. 6.2.4.2 vereinbarten Zeiten angenommen.

☐ Zusätzlich werden Störungsmeldungen während folgenden Zeiten angenommen:

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

9 Erfüllungsort

Soweit nicht an anderer Stelle für einzelne Leistungen bereits vereinbart:

Himmelshafen, Sitz des Auftraggebers

10 Verantwortlicher Ansprechpartner

des Auftraggebers:	Frau Himmelszorn, Dezernent für Informations- und Kommunikationstechnik
des Auftragnehmers:	Herr Gottesblitz, Vertriebsleiter Europa

11 Mitwirkungsleistungen des Auftraggebers

☐ Folgende Mitwirkungsleistungen (z. B. Infrastruktur, Organisation, Personal, Technik, Dokumente) werden vereinbart:

12 Schlichtungsverfahren

☐ Die Anrufung folgender Schlichtungsstelle wird vereinbart:

13 Kündigung (abweichend von Ziffer 4.1 EVB-IT Pflege S)

☐ Es wird eine Kündigungsfrist von Monaten vereinbart.

14 Versicherung

☒ Der Auftragnehmer weist nach, dass die Haftungshöchstsummen gemäß Ziffer 10.2.1 EVB-IT Pflege S durch eine Versicherung abgedeckt sind, die im Rahmen und Umfang einer marktüblichen deutschen Industriehaftpflichtversicherung oder einer vergleichbaren Versicherung aus einem Mitgliedsstaat der EU entspricht.

15 Sonstige Vereinbarungen

- Der Gerichtsstand ist Himmelshafen.
- Sämtliche Leistungen werden nach dem Stand der Technik bei Leistungserbringung erbracht.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Auftragsdatenverarbeitungs-Vertrag (ADV-Vertrag)

Präambel

Die Vertragsparteien sind sich darüber einig, dass in diesem Auftragsdatenverarbeitungsvertrag („ADV-Vertrag“) nur datenschutzrechtliche Regelungen zur Auftragsdatenverarbeitung getroffen werden. Gleichwohl gelten bei der Verarbeitung von Patientendaten die strafrechtlichen Bestimmungen, die aus §203 StGB resultieren. Die Verantwortung für die Wahrung der ärztlichen Schweigepflicht obliegt dem Auftraggeber, da diese Verantwortung ebenso wenig wie die datenschutzrechtliche Verantwortung vom Auftraggeber an den Auftragnehmer delegiert werden kann. Der Auftragnehmer sichert dem Auftraggeber zu, dass er bei der Verpflichtung des von ihm eingesetzten Personals auf das Datengeheimnis auf die hohe Schutzwürdigkeit von Patientendaten sowie auf die eventuell aus dem Gesetz gegen den unlauteren Wettbewerb resultierenden strafrechtlichen Folgen einer unbefugten Offenbarung hinweist.

Dieser ADV-Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag „EVB-IT Pflegevertrag S“ (im folgenden Hauptvertrag genannt) beschriebenen Auftragsdatenverarbeitung ergeben. Die beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend §2 und §3 BDSG, §2 UWG und §2 TMG sowie Landesdatenschutzgesetz NRW und das Gesundheitsdatenschutzgesetz NRW. Sollten in den Paragraphen sich widersprechende Darstellungen finden, gelten die Definitionen in der Reihenfolge BDSG, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(2) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Gegenstand, Verantwortlichkeit und Dauer des Auftrags

§2.1 Gegenstand des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der darin enthaltenen Leistungsbeschreibung konkretisiert sind. Im Einzelnen sind insbesondere folgende Daten Bestandteil der Datenverarbeitung:

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Art der Daten	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen
SAP, Krankenhaus-Verwaltungssoftware	Unterstützung des Auftraggebers bei der Betreuung des eingesetzten SAP-Systems	Personenstammdaten
Internetdaten (E-Mail)	Wartung des vom Auftraggeber eingesetzten Mailservers	Kommunikationsdaten Personaldaten
Internetdaten (z.B. WWW, FTP, E-Mail)	Betreuung der vom Auftraggeber eingesetzten Firewall	Kommunikationsdaten Personaldaten
Daten aus dem Krankenhausinformationssystem	Wartung des eingesetzten KIS	Patientendaten

§2.2 Verantwortlichkeit

(1) 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 („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

(3) Die Inhalte dieses ADV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§2.3 Dauer des Auftrags

(1) Die Laufzeit dieses ADV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses ADV-Vertrages nicht darüber hinausgehende Verpflichtungen ergeben.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen ADV-Vertrages keine Auftragsdatenverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform

§2.4 Weisungsbefugnis des Auftraggebers

1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.
3. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

2.5 Leistungsort

1. Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen.
2. Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem anderen Standort im Ausland erbringen möchte, wird der Auftragnehmer die schriftliche Bestätigung durch den Auftraggeber einholen.
3. Entsprechendes gilt für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.
4. Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) 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 zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen der entsprechenden datenschutzrechtlichen Bestimmungen (Bundesrecht, Landesrecht sowie ggfs. Kirchenrecht) entsprechen. Dies beinhaltet insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen entsprechend §9 BDSG sowie §78a SGB X hinsichtlich der

   a) Organisationskontrolle,
   b) Zutrittskontrolle,
   c) Zugangskontrolle,
   d) Zugriffskontrolle,
   e) Weitergabekontrolle,
   f) Auftragskontrolle,
   g) Verfügbarkeitskontrolle sowie des
   h) Trennungsgebots.

   Eine Maßnahme nach b bis d ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

   Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Achtung: Dies ist nur ein Beispiel und in keiner Form für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird Anhang zu diesem Vertrag.

(3) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung.

(4) Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG sowie §88 TKG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichten und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren. Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftraggebers zu verpflichten und müssen auf §17 UWG hingewiesen werden. Weiterhin müssen die vom Auftragnehmer eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

Eine gesetzliche Offenbarungspflicht des Auftragnehmers bleibt hiervon unberührt.

(5) Der Auftragnehmer bestellt einen Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f bis 4g BDSG ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer … bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.

(7) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

(8) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

(10) Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(11) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze 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 bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

(12) (14) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(13) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(14) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

(15) Der Auftragnehmer unterwirft sich entsprechend §11 BDSG sowie den entsprechenden landesrechtlichen bzw. kirchlichen Bestimmungen hinsichtlich der Kontrolle bzgl. der dieser Vereinbarung zugrunde liegenden Datenverarbeitung der Kontrolle durch die für den Auftraggeber zuständige Aufsichtsbehörde.

(16) 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 Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

(17) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

§3.1 Fernzugriff bei Prüfung/Wartung eines Systems

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen gelten ergänzend folgende Regelungen:

1. Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / betroffenen Mitarbeiter des Auftraggebers durchgeführt.
2. Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagenwerden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.
3. Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.
4. Vor Durchführung von Fernzugriffen zu Zwecken von Prüfungs- und/oder Wartungsarbeiten werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherungsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.
5. Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
6. Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfange – auch in zeitlicher Hinsicht - Gebrauch machen, als

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

7. Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions- /Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.
8. Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
9. Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

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

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat dementsprechend die Pflicht zur Führung des Verfahrensverzeichnisses.

(4) Dem Auftraggeber obliegen die aus § 42a BDSG und §15a TMG resultierenden Informationspflichten.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 5 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

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.

(2) 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.

(3) Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

(4) Soweit nicht ausdrücklich vereinbart, wird der Aufwand der Löschung gesondert vergütet. Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

§ 6 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig [alternativ ist ein Zeitraum festzulegen] von der Einhaltung der in diesem ADV-Vertrag vereinbarten Regelungen zum Schutz der personenbezogenen bzw. personenbeziehbaren Daten, insbesondere von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

Hierfür kann er beispielsweise

- Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen oder
- nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer muss auch hierbei weitestgehend vermieden werden.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

§ 7 Unterauftragnehmer

(1) Eine Weitergabe von Aufträgen der im Hauptvertrag vereinbarten Tätigkeiten an Unterauftragnehmer durch den Auftragnehmer erfolgt nicht.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

(2) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.
(3) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.
(4) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie in diesem ADV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers.
(5) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
(6) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen.
(7) Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.
(8) Unter-Unterauftragsverhältnisse sind analog den Vorgaben zu Unterauftragsverhältnissen datenschutzrechtlich zu gestalten.
(9) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

§ 8 Individualvertragliche Ergänzung

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 10 Schriftformklausel

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung 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.

§ 11 Salvatorische Klausel

1. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

2. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
3. Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
4. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter §11 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 12 Erfüllungsort

Erfüllungsort ist der Ort des Auftraggebers.

§ 13 Rechtswahl, Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.

§14 Anlage(n)

- Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe
- Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen entsprechend §9 BDSG bzw. der Anlage zu BDSG § 9 Satz 1.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

Anhang 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Zur Zeit werden keine Unterauftragnehmer eingesetzt.

Anhang 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen zur Fernwartung

1) Zutrittskontrolle

Dieser Abschnitt bezieht sich auf Gebäude, Räume und technische Anlagen, von denen aus die Fernwartung durchgeführt wird und die sich nicht im Verantwortungsbereich des Auftraggebers befinden.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

1. Es besteht eine für alle Personen verbindliche Zugangsauthentisierung durch eine reglementierte Vergabe von Schlüsseln, ohne die ein Zutritt nicht möglich ist.
2. Einen Schlüssel erhält nur, wer aufgrund der Zugehörigkeit zur. Gruppe der Fernwartenden gehört.
3. Die Vergabe der Schlüssel wird dokumentiert.
4. Außerhalb der Betriebszeiten werden die Räumlichkeiten durch eine Alarmanlage geschützt, die mit einem Pförtner verbunden ist. Der Pförtner kann im Bedarfsfall unverzüglich die Polizei informieren.

2) Zugangskontrolle

Es existieren folgende Maßnahmen zur Zugangskontrolle:

1. Authentifizierungsmedien sowie Zugangskennungen werden grundsätzlich personengebunden vergeben und nicht an Dritte weitergegeben.
2. Zur Authentisierung existieren Passwortkonventionen.
    a. Die Vorgabe für die Passwortmindestlänge ist 8 Zeichen.
    b. Es muss bei der Passwortvergabe sowohl die Groß- wie auch die Kleinschreibung verwendet werden, weiterhin muss mindestens eine Ziffer und ein Sonderzeichen verwendet werden.
    c. Trivialpasswörtern wie der eigene Name sind verboten.
    d. Das Passwort muss nach Ablauf einer Frist von 180 Tagen geändert werden.
3. Zugriffspasswörter und/oder Formulareingaben werden nicht auf dem Rechner gespeichert, sondern müssen immer von dem Fernwartenden eingegeben werden.
4. Es werden ausschließlich verschlüsselte Netzwerkverbindungen zur Fernwartung genutzt.
5. Alle erfolgreichen und abgewiesenen Zugangsversuche werden protokolliert:
    a. verwendete Kennung,
    b. Rechner, der zur Fernwartung benutzt wurde
    c. IMEI, IP- oder Macadresse.

    Auf Aufforderung des Kunden kann jederzeit eine Auswertung erfolgen.

3) Zugriffskontrolle

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

1. Jeder Zugriff auf etwaige lokal abgelegte Zwischenspeicher oder Datenbanken, die Kundendaten des Auftraggebers enthalten, die der Auftraggeber nicht freigegeben oder bereitgestellt hat, unterbleibt.

Achtung: Dies ist nur ein Beispiel und in keiner Form für den Einsatz in einer realen Vertragsbeziehung vorgesehen

2. Es gibt Regelungen und Verfahren zum Anlegen, Ändern und Löschen von Berechtigungsprofilen bzgl. der Fernwartung.
3. Der Umfang der Berechtigungen innerhalb der Fernwartungsprofile wird dabei auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum beschränkt. Berechtigungen sind dabei immer an eine persönliche Benutzerkennung und an einen Account geknüpft.
4. Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist beim Auftragnehmer eingeführt. Entfällt die Grundlage für eine Berechtigung (z. B. Funktionsänderung), wird diese sofort entzogen.
5. Zugriffe auf die personenbezogenen Daten und Berechtigungen werden zeitlich begrenzt vergeben.
6. Soweit Datenbestände mehrerer Auftraggeber in einer Datenbank gespeichert sind oder mit einer Datenverarbeitungsanlage verarbeitet werden, ist eine logische Zugriffseinschränkung implementiert, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet ist (Mandantenfähigkeit).

4) Weitergabekontrolle

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

1. Es werden keine Daten des Auftraggebers außerhalb der EU erhoben oder verarbeitet.
2. Eine Weitergabe der Daten des Auftraggebers erfolgt ausschließlich auf Weisung des Auftraggebers. Dabei wird immer im jeweiligen Einzelfall gemeinsam mit dem Auftraggeber festgelegt, an wen welche Daten übermittelt werden sollen und auf welchem Übertragungsweg dies zu geschehen hat.
3. Die Datenübertragungen zwischen Clients und Servern erfolgt dabei ausschließlich verschlüsselt, dabei erfolgt bei jeder Datenübertragung beim Auftragnehmer eine Protokollierung. Falls möglich erfolgt auch beim Empfänger eine Protokollierung, sodass sendende und empfangende Stelle protokollieren.
4. Beim Auftraggeber sind ständig aktivierte Hardware-Firewalls im Einsatz, die durch den Nutzer nicht deaktivierbar sind.
5. Temporäre Zwischenspeicher (z. B. der Browsercache oder der TEMP-Ordner des Betriebssystems) sind so konfiguriert, dass ihre Inhalte regelmäßig automatisiert gelöscht werden.
6. Es gibt Regelungen zur datenschutzkonformen Vernichtung von Dokumenten und Datenträgern. Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit Kundendaten des Auftraggebers wird protokolliert; das Protokoll wird dem Auftraggeber auf Nachfrage zur Verfügung gestellt.

5) Eingabekontrolle

Es existieren folgende Maßnahmen zur Eingabekontrolle:

1. Es existiert eine Dokumentation, welche Personen aufgrund ihrer Aufgabenstellung befugt und verantwortlich sind, Eingaben in der Datenverarbeitungsanlage vorzunehmen.
2. Die Eingaben personenbezogener Daten in die Datenverarbeitungsanlage werden protokolliert.
3. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Auftraggeber vereinbarten Regelungen. Bei fehlenden Regelungen ist von 6 Monaten auszugehen.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen

6) Auftragskontrolle

Es existieren folgende Maßnahmen zur Auftragskontrolle:

1. Weisungsbefugte Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt.
2. Desgleichen sind zur Entgegennahme und Ausführung von Weisungen des Auftraggebers befugte Personen benannt und dem Auftraggeber bekannt.
3. Der Kreis der zur Fernwartung autorisierten Personen beim Auftragnehmer wurde auf das zur Aufgabenerfüllung notwendige Minimum beschränkt.
4. Die zulässigen Orte, von denen eine Fernwartung durchgeführt werden kann, wurden festgelegt. Die Festlegung wurde dokumentiert und ist Teil der Verfahrensbeschreibung.
5. Der Auftraggeber stellt verfahrenstechnisch eine Kontrolle Aufträge sicher.
6. Es erfolgt beim Auftragnehmer eine Protokollierung der Fernwartung. Auf Anforderung des Auftraggebers kann der Auftragnehmer belegen, dass der jeweilige Auftrag nach den Weisungen des Auftraggebers durchgeführt wurde. Die Protokollierung enthält
    a. die beauftragenden Kontaktperson des Auftraggebers (Name, Abteilung)
    b. die genaue Spezifikation der des Auftrags
    c. Angaben zur Terminierung seitens des Aufraggebers
7. Ist eine Datenübertragung unabdingbar, wird die Übertragung nur nach vorheriger schriftlicher Einwilligung des Auftraggebers und nur bei gleichzeitiger Protokollierung der übertragenen Daten durchgeführt.

7) Verfügbarkeitskontrolle

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

1. Es existiert ein Notfallplan, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen, insb. auch auf Seite des Auftraggebers, über den Vorfall zu unterrichten sind.
2. Es findet eine regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter statt.
3. Es existiert ein Backup-Konzept und eine für das Backup verantwortliche Person und Vertreter sind benannt.

8) Trennungskontrolle

Es existiert folgende Maßnahmen zur Trennungskontrolle:

1. Es werden nur solche Daten erhoben, gespeichert oder verarbeitet, die zur Erfüllung der Aufgabe oder Durchführung des Wartungsauftrages unbedingt notwendig sind.

Achtung: Dies ist nur ein Beispiel und nicht für den Einsatz in einer realen Vertragsbeziehung vorgesehen