

# Vertrag über die Auftragsdatenverarbeitung personenbezogener Daten (ADV-Vertrag)

zwischen

---

---

---

---

im folgenden **Auftraggeber** genannt und der

KBS - Kaufmännisches Beratungs-  
und Servicebüro GmbH  
Jänickendorfer Straße 58  
15518 Steinhöfel

im folgenden **Auftragnehmer** genannt.

## 1 Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
- (3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

## 2 Gegenstand und Dauer der Verarbeitung

### 2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen / Supportleistungen:

- Fernwartungen
- EDV-Dienstleistungen mit Zugang zu personenbezogenen Daten (auch vor Ort)
- Übernahme von Mandantensicherungen zur Bearbeitung von Supportanfragen

### 2.2 Dauer

Die Verarbeitung beginnt mit dem Datum der Unterzeichnung dieses Vertrages durch den Auftraggeber und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

## 3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

### 3.1 Art und Zweck der Verarbeitung

Die Verarbeitung durch den Auftragnehmer ist folgender Art:

- Überprüfen/Bearbeiten von Programminstallation und/oder -Anwendungen
- Überprüfen/Bearbeiten von Hardwarekomponenten und/oder -Systemen
- Überprüfen/Bearbeiten von Daten kaufmännischer oder sonstiger Anwendungen

Folgende Datenarten sind dabei regelmäßig Gegenstand der Verarbeitung: Daten aus kaufmännischen Anwendungen wie: Handwerkersoftware, Zeiterfassung, Document Management System, Auftragsbearbeitung, Finanzbuchhaltung, Lohn & Gehalt, CRM u.a.

Die Verarbeitung dient folgendem Zweck: Sicherstellung der Arbeitsfähigkeit der EDV des Auftraggebers durch EDV-Dienstleistungen und EDV-Support des Auftragnehmers.

### 3.2 Art der Daten

Folgende Daten sind betroffen: personenbezogene Daten des Auftraggebers, sowie die personenbezogenen Daten von Kunden, Lieferanten und Mitarbeitern des Auftraggebers.

#### 3.2.1 Kreis der von der Datenverarbeitung betroffenen Personen

Von der Verarbeitung betroffen sind Kunden, Lieferanten und Mitarbeitern des Auftraggebers.

## 4 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

- (7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
- (11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

## 5 Technische und organisatorische Maßnahmen

- (1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- (6) Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an

Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

- (7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

## 6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

## 7 Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist nur mit Zustimmung des Auftraggebers zugelassen.
- (2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- (4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- (6) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtung vollständig erfüllt (Auftragsdatenverarbeitungsvertrag mit dem Subunternehmer).
- (7) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
- (8) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Subunternehmer gelten. Es ist zudem vertraglich zu regeln, dass der Subunternehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

- (9) Zurzeit sind die in Anlage 2 mit Namen und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
- (10) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

## 8 Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
- (5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

## 9 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
  - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
  - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

- d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

## 10 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.
- (3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (4) 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.

## 11 Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung bleiben unberührt.
- (2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Kontrolle der Datenverarbeitungsanlage in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.
- (3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen gesetzlichen Aufbewahrungsfristen entsprechend, auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

## 12 Vergütung

Die Vergütung des Auftragnehmers ist gesondert geregelt. Eine Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

## 13 Haftungsbeschränkung

Keine Haftung für Folgeschäden – Weder der Auftragnehmer noch die Subunternehmer sind für irgendwelche Schäden ersatzpflichtig, die auf Grund einer Verletzung der Pflichten dieses Vertrages entstehen. Dieser Ausschluss gilt nicht für Schäden, die durch Vorsatz Seitens des Auftragnehmers oder seiner Subunternehmer verursacht wurden. Ebenfalls bleiben die gesetzlichen Regeln des Art. 82 DSGVO davon unberührt.

## 14 Kündigung und Sonderkündigungsrecht

- (1) Dieser Vertrag ist mit einer Frist von drei Monaten zum Quartalsende kündbar.
- (2) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

## 15 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

### Auftraggeber

\_\_\_\_\_, den \_\_\_\_ . \_\_\_\_ . \_\_\_\_

\_\_\_\_\_  
Name / Funktion

### Auftragnehmer

Steinhöfel, den 01.05.2018

Hübner / Geschäftsführer



**KBS**  
Kaufmännisches Beratungs- und Servicebüro GmbH  
Jänickendorfer Str. 58, 15518 Steinhöfel OT Buerfelde  
Tel.: 033637/3105 Fax: 033637/3104  
E-Mail: info@kbsgmbh.de / Internet: www.KBSGmbH.de

\_\_\_\_\_  
Unterschrift und Stempel

\_\_\_\_\_  
Unterschrift und Stempel

# Anlage 1

## Technische und organisatorische Maßnahmen des Auftragnehmers gemäß § 9 BDSG

### **1. Zutrittskontrolle zu den Geschäftsräumen**

- 1 Hoftor mit Sicherheitsschloss
- 2 massive Eingangstüren mit Sicherheitsschlössern
- Schlüsselregelung

### **2. Zugangskontrolle zur Datenverarbeitungsanlage**

- Zuordnung von Benutzerrechten
- Nutzung von Passwörtern auf allen Computern
- Einsatz der Anti-Viren Software GDATA AntiVirus (Bezahlversion) auf allen Computern
- Einsatz der Windows-Firewall auf allen Computern
- Einsatz der Hardware-Firewall des DSL-Routers

### **3. Zugriffskontrolle**

- Verwaltung der Rechte durch Systemadministrator (2 Administratoren)
- Nutzung von Passwörtern
- Sichere Aufbewahrung externer Datenträger außerhalb der Geschäftsräume
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von temporären Datenträgern (CD, DVD)
- Einsatz von Aktenvernichtern

### **4. Weitergabekontrolle**

- Vermeidung von Datentransporten per eMail
- Nutzung passwortgeschützter Downloads für den elektronischen Datentransport
- Beim physischen Transport von Akten und Datenträgern: Verwendung sicherer Transportverpackungen und sorgfältige Auswahl von Transportpersonal und -fahrzeugen

### **5. Eingabekontrolle**

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Zuordnung von Aufgaben an namentlich benannte Verarbeiter
- Führung eines Verfahrensverzeichnisses

### **6. Auftragskontrolle**

- Auswahl der Mitarbeiter des Auftragnehmers unter Sorgfaltspflicht
- Datenschutzbelehrung aller Mitarbeiter des Auftragnehmers
- Sicherstellung und Dokumentation der Vernichtung der Daten nach Auftragsbeendigung
- Kontrollrechte gegenüber Auftragnehmer in diesem AV-Vertrag vereinbart

### **7. Verfügbarkeitskontrolle**

- Geprüftes Feuerlöschgerät in der Betriebsstätte
- Verwendung eines Backup- und Recoverykonzepts
- Regelmäßige Tests der Datenwiederherstellung
- Sichere Aufbewahrung der Datensicherung an einem ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

### **8. Trennungsgebot**

- Softwareseitige logische Mandantentrennung
- Festlegung von Datenbank- und Programmrechten
- Physische Trennung von Produktiv- und Testsystemen

## Anlage 2

# Zugelassene Subdienstleister

**Der Auftragnehmer nimmt für Dienstleistungen, Registrierungen oder Lizensierungen im Auftrag des Auftraggebers, Leistungen von Subdienstleistern in Anspruch, die in seinem Auftrag Daten verarbeiten. Dabei handelt es sich um folgende deutsche Unternehmen, die ebenfalls den gesetzlichen Bestimmungen zum Datenschutz unterliegen:**

- blue:solution Software, Helmerich PCAS, sage Software und Gejatec GmbH – Zweck: Lizensierung beim Kauf von kaufmännischer Bürosoftware und Fernwartung der Bürosoftware beim Auftraggeber, sowie im Einzelfall die Überprüfung von Mandantensicherungen zur Bearbeitung von Supportanfragen
- G DATA Software AG – Zweck: Registrierung von Anti Viren Software
- ratiokontakt GmbH – Zweck: Domain-Registrierung und WEB-Hosting

# Anlage 3

## Weisungsberechtigte und Weisungsempfangsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

### **Beim Auftraggeber:**

- Mitarbeiter aus der Geschäftsführung (bei Bedarf weitere Mitarbeiter namentlich benennen)

---

---

---

### **Beim Auftragnehmer:**

- Mitarbeiter der Geschäftsführung (Herr Hübner)
- Mitarbeiter aus Support und Administration (Herr Hoffmann, Herr Plagemann)
- Sachbearbeiter aus der Lohn- und Finanzbuchhaltung (Frau Brosinsky)