

# Vertrag über die Auftragsverarbeitung personenbezogener Daten

## 1. Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und a.b.s. (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter von a.b.s. 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 Gegenstand der Verarbeitung ist im Dienstleistungsabkommen (im Folgenden „Hauptvertrag“) exakt beschrieben.

### 2.2 Dauer

Die Verarbeitung beginnt und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei. Die Kündigungsfristen sind die des Hauptvertrages.

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

### 3.1 Art und Zweck der Verarbeitung

Die Verarbeitung dient dem Zweck, den Hauptvertrag zu erfüllen. Hierzu werden vom Auftraggeber personenbezogene Daten seiner Mitarbeiter zur Verarbeitung zu Verfügung gestellt mit dem Ziel, die monatliche Lohn- und Gehaltsabrechnung zu fertigen, die Meldungen an die Sozialversicherungsträger und das Finanzamt zu tätigen sowie die notwendigen Überweisungen zu erstellen. Die Daten werden nach der Verarbeitung gespeichert, um Jahresauswertungen erstellen zu können oder auch Rücksicherungen durchführen zu können.

### 3.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Alle für die Lohn- und Gehaltsabrechnung relevanten Daten

### 3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Alle Mitarbeiter, die vom Hauptvertrag betroffen sind.

## 4. Pflichten von a.b.s.

- (1) a.b.s. verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, a.b.s. ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für a.b.s. bestehen, teilt a.b.s. diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist a.b.s. gesetzlich verboten. a.b.s. verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) a.b.s. bestätigt, dass a.b.s. die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. a.b.s. beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) a.b.s. 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) a.b.s. sichert zu, dass die bei a.b.s. 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. a.b.s. trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernungen laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat a.b.s. 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 a.b.s. den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf a.b.s. nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an a.b.s. gerichtete Anfragen wird a.b.s. unverzüglich an den Auftraggeber weiterleiten.
- (9) Soweit gesetzlich verpflichtet, bestellt a.b.s. 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. a.b.s. 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 a.b.s. 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 a.b.s. nicht in der Europäischen Union niedergelassen, bestellt a.b.s. 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 von a.b.s. 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 a.b.s. 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 a.b.s. den Auftraggeber unverzüglich.
- (4) a.b.s. 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 nicht 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.
- (8) a.b.s. führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

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

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

## 7. Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall 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 a.b.s. 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 von a.b.s. und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- (6) a.b.s. wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- (7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich a.b.s. dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. a.b.s. hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
- (8) 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. a.b.s. teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
- (9) a.b.s. hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.
- (10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür a.b.s. gegenüber dem Auftraggeber.
- (11) Zurzeit sind die in Anlage 2 mit Namen, Anschrift 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 von a.b.s. gegenüber Subunternehmern bleiben unberührt.
- (12) 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 von a.b.s., 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 a.b.s. 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 bei a.b.s. 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 von a.b.s. **soweit erforderlich** Zutritt und Einblick zu ermöglichen. a.b.s. ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Die hierfür bei a.b.s. entstehenden Kosten für Personalaufwand und ggf. Produktionsausfall hat der Auftraggeber zu übernehmen.
- (5) Kontrollen bei a.b.s. haben ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten von a.b.s., sowie nicht häufiger als alle 12 Monate statt. Soweit a.b.s. den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

## 9. Mitteilungspflichten

- (1) a.b.s. teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten aus dem Auftragsverhältnis unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis von a.b.s. 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 von a.b.s. 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 Auftragserledigung sowie Verstöße von a.b.s. oder der bei a.b.s. beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) a.b.s. informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) a.b.s. 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 a.b.s. benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen.
- (3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (4) a.b.s. wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. a.b.s. ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (5) a.b.s. hat erteilte Weisungen und deren Umsetzung zu dokumentieren.

## 11. Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat a.b.s. 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. Eine physische Vernichtung erfolgt gemäß DIN 66399.
- (2) a.b.s. ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
- (3) a.b.s. hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- (4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch a.b.s. den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. a.b.s. kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

## 12. Vergütung

Die Vergütung von a.b.s. ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt vorbehaltlich des §8(4) nicht.

## 13. Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und a.b.s. als Gesamtschuldner gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.
- (2) a.b.s. trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von a.b.s. zu vertretenden Umstandes ist, soweit die relevanten Daten von a.b.s. unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt a.b.s. den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt a.b.s. dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

# Vertrag über die Auftragsverarbeitung personenbezogener Daten

- (3) a.b.s. haftet dem Auftraggeber für Schäden, die a.b.s. seine Mitarbeiter bzw. die von a.b.s. mit der Vertragsdurchführung Beauftragten oder die von a.b.s. eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
- (4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

## 14. Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß von a.b.s. gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, a.b.s. eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder a.b.s. Kontrollrechte des Auftraggebers vertragswidrig verweigert.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn a.b.s. die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (3) Bei unerheblichen Verstößen setzt der Auftraggeber a.b.s. eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

## 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. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers bei a.b.s. durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat a.b.s. 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 dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

## 16. Wirksamkeit des Vertrages

**Dieser Vertrag über die Auftragsdatenverarbeitung personenbezogener Daten und dessen Anlagen erreichen Wirksamkeit mit der Unterschrift des Dienstleistungsabkommens vom \_\_\_\_\_ und sind damit Bestandteil dieses Dienstleistungsabkommens.**

## Anlagen

### Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die a.b.s. mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

1. Unsere Eingänge sind mit Schleusen versehen, so dass ein unberechtigtes Eindringen unmöglich gemacht wird (Siehe Prüfbericht des Tüv's vom 23.11.1993) Seit der Prüfung wurden keinerlei baulichen Veränderungen vorgenommen.
2. Sämtliche Verbindungen unseres Systems sind mittels Firewalls nach dem neuesten Stand der Technik abgeschottet. Die Email-Übertragung läuft über einen Stand-Alone-PC, der ebenfalls über Firewall abgesichert ist. Eine Sammlung der Email erfolgt im 5-Minuten-Abstand, die Verteilung in das Abrechnungssystem erfolgt nur in eine Richtung, nämlich durch Zugriff der EDV-Anlage zum Stand-Alone System.
3. Schreibzugriff zu personenbezogenen Daten haben nur autorisierte Personen. Dies sind unsere Programmierer. Alle anderen Mitarbeiter haben Lesezugriff, der sich aus der Logik unserer Tätigkeit ergibt.
4. Die Weitergabe unserer Daten erfolgt auf Basis einer Verschlüsselung nach RC4 mit 128bit Schlüssel. Der Schlüssel ist nur auf den Kundenrechner und im Rechenzentrum hinterlegt.
5. Jedweder Datenaustausch zwischen den Kunden und a.b.s. ist kontrolliert und abgespeichert. Sämtliche zur Durchführung notwendigen Tätigkeiten, wie das Anstoßen der Abrechnung, des Druckes oder der Datensicherung erfolgt vollautomatisch und wird ebenfalls dokumentiert. Bei von a.b.s. erfassten Daten wird genau festgehalten, wer, wann welche Daten eingegeben hat.
6. Bei Daten der Kunden, die mit unserer Software LobuOnline arbeiten, haben wir keinerlei Zugriffsmöglichkeiten. Insofern werden diese ohnehin nach Weisung des Auftraggebers verarbeitet. Daten, die von Kunden per Papier hereingegeben werden, werden von einer Datentypistin erfasst und von einer anderen geprüft. Das gleichzeitige Erfassen und Prüfen desselben Auftrages wird durch das System unterbunden.
7. Unsere Festplatten werden nach RAID 10, d.h. RAID 1 (Plattenspiegelung 1 :1) und Raid 0 (Platten-Spanning, d.h. Verteilung der Daten auf mehreren Platten) gesichert, die Daten werden über das Netzwerk auf einem zweitem Rechner gespiegelt. Darüber hinaus werden die Daten auf Magnetbändern gesichert und archiviert.
8. Die Daten werden jeweils zu den für ihren Zweck bestimmten Ablauf eingesetzt und verarbeitet, damit ist auch eine getrennte Verarbeitung möglich und gewährleistet. Darüber hinaus hat jeder Mitarbeiter der a.b.s. Rechenzentrum GmbH eine entsprechende Datenschutzverpflichtungserklärung unterzeichnet.
9. Ein ausgeklügeltes Backup-Verfahren ermöglicht uns eine Wiederanlaufzeit von ca. 4 Stunden nach einem Totalausfall (Brand/Wasser/sonstige Zerstörung der Anlagen).
10. Die Räume der Firma a.b.s. sind durch Alarmanlage mit Bewegungs-, Glasbruch- und Rauchmeldern abgesichert. Die Eingänge zur Straße sind durch Schleusen und einem großen Stehltor gesichert, das nur zu den Betriebszeiten der Firma a.b.s. frei zugänglich ist. Außerhalb müssen Besucher, die zu anderen Mietern im Geschäftshaus wollen, klingeln.

### Anlage 2 - Zugelassene Subdienstleister

Ausdrücklich werden keine Subdienstleister zugelassen.