Datenschutz; Stand: 24.04.2008

Beispiel eines Mustervertrags zur Auftragsdatenverarbeitung

Nachfolgend wurde ein Mustervertrag für die Verarbeitung personenbezogener Daten im Auftrag entworfen, der allerdings möglichst universell gehalten ist und insbesondere an den verschiedenen, besonders gekennzeichneten Stellen noch aufgabenspezifisch anzupassen ist. Der Mustervertrag erhebt keinen Anspruch auf Vollständigkeit.

Die kursiv gehaltenen Texte sind durch eigene Angaben zu ersetzen.

Vereinbarung

zwischen .....

(Name der Behörde)

- nachstehend Auftraggeber genannt -

und .....

(Name der beauftragten Stelle)

- nachstehend Auftragnehmer genannt -

§ 1 Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

Der Auftrag umfasst folgende Arbeiten:

(*Genaue Definition der Aufgaben und der vom Auftragnehmer zu erbringenden Leistungen*)

für folgende Zwecke:

(detaillierte Beschreibung der Zwecke der Auftragsdatenverarbeitung)

§ 2 Rechte und Pflichten des Auftraggebers

1. Für die
   - Beurteilung der Zulässigkeit der Datenverarbeitung,
   - die Wahrung der Rechte der Betroffenen,
   - die datenschutzrechtliche Freigabe,
   - die Führung des Verfahrensverzeichnisses und
   - die Einhaltung der sonstigen gesetzlichen Datenschutzvorschriften

   ist allein der Auftraggeber verantwortlich. Er wird dabei vom Auftragnehmer auf Verlangen unterstützt.
2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich.
3. Der Auftraggeber legt die technischen und organisatorischen Maßnahmen nach Art. 7

BayDSG fest, die im Rahmen der Auftragsdatenverarbeitung einzuhalten sind. Generell ist

1. Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogene Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Dabei sind insbesondere folgende Maßnahmen zu ergreifen:
(Anmerkung: Eine ***detaillierte*** *Beschreibung der zu ergreifenden technisch-organisatorischen Datenschutz- und Datensicherheitsmaßnahmen kann sowohl hier erfolgen als auch in einer Anlage beigefügt werden)*

- ausschließliche Verwendung ausgetesteter und datenschutzrechtlich freigegebener DV-Programme
- Ergreifung von Maßnahmen zur Vollständigkeitskontrolle
- Einsatz von Sicherheitsmaßnahmen nach dem Stand der Technik
- zugriffssichere Speicherung und Aufbewahrung der Daten
- Maßnahmen zur Identifizierung und Authentifizierung
- Sicherheitsmaßnahmen im Rahmen einer Datenübertragung (z. B. Call-back-Verfahren, Verschlüsselung)
- Protokollierung und Auswertung von Protokolldaten insbesondere hinsichtlich von Sicherheitsverletzungen
- Maßnahmen zur Katastrophenvorsorge

4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten

Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, die ihm im Rahmen der Auftragsdatenverarbeitung bekannt gewordenen personenbezogenen Daten des Auftraggebers geheim zu halten und alle in §2 vereinbarten Sicherheitsmaßnahmen zu ergreifen.
2. Die dabei im Einzelnen ergriffenen bzw. zu ergreifenden Maßnahmen werden in einem Sicherheitskonzept festgelegt, das dem Auftraggeber zur Verfügung gestellt wird. Dieses Sicherheitskonzept wird laufend überprüft und (dem technischen Fortschritt) angepasst.
3. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit dazu berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der von ihm getroffenen Weisungen zu überprüfen. Dies gilt auch für die Betretung einer Privatwohnung im Falle der Telearbeit. Der Auftragnehmer gewährleistet das für die Durchführung der Kontrollen erforderliche Betretungsrecht, die Einsichtnahme in diesbezügliche Unterlagen, die Vorführung der im Rahmen der Auftragsdatenverarbeitung betrieblichen Abläufe und unterstützt das mit der Durchführung der Kontrolle beauftragte Personal hinsichtlich ihrer Tätigkeit.
4. Der Auftragnehmer setzt für die auftragsgemäße Verarbeitung personenbezogener Daten nur Personal ein, das
    - auf das Datengeheimnis nach § 5 BDSG und nach dem Verpflichtungsgesetz verpflichtet wurde,
    - über die Regelungen der Datenschutzgesetze sowie sonstigen datenschutzrechtlichen Vorgaben angemessen und der Aufgabensituation entsprechend belehrt und geschult wurde und
    - über genügend Sachkunde für die ordnungsgemäße Abwicklung der Aufgaben verfügt.
5. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach den Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.
6. Der Auftragnehmer gewährleistet - soweit gewünscht - eine Protokollierung der Aktivitäten.
7. Anfallendes Test- und Ausschussmaterial wird vom Auftragnehmer unter Verschluss gehalten, bis es entweder vom Auftragnehmer datenschutzgerecht vernichtet oder dem Auftraggeber übergeben wird. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten dürfen erst nach Weisung durch den Auftraggeber datenschutzgerecht vernichtet werden. Entsprechende Löschprotokolle sind dem Auftraggeber auf Verlangen auszuhändigen.
8. Nach der Beendigung seiner diesbezüglichen Tätigkeit hat der Auftragnehmer alle Daten und überlassene Datenträger (einschließlich etwaig angefertigter Kopien) an den Auftraggeber heraus- bzw. zurückzugeben oder auf dessen Verlangen datenschutzgerecht zu löschen.
9. Die Verarbeitung von personenbezogenen Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet.
10. Eventuelle Aufträge an Subunternehmer (auch zu Zwecken der Wartung bzw. Fernwartung) dürfen nur nach vorheriger schriftlicher Genehmigung durch den Auftraggeber vergeben werden. Bei der Einschaltung von Subunternehmen gelten für

diese die gleichen Pflichten wie für den Auftragnehmer. Dieser hat die Einhaltung der Pflichten regelmäßig zu überprüfen.
Ein Vertrag mit einem Subunternehmer ist ebenfalls schriftlich zu fixieren. Der entsprechende Vertrag ist dem Auftraggeber vorzulegen.

11. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei Prüfungen durch die Datenschutzaufsichtsbehörde, schwer wiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
12. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich darüber, 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 der Auftraggeber eine Entscheidung darüber getroffen hat.
13. Verlangt ein Dritter die Herausgabe bzw. Bekanntgabe von Daten, die im Rahmen der Auftragsdatenverarbeitung erhoben, verarbeitet oder genutzt werden, leitet der Auftragnehmer das diesbezügliche Begehren an den Auftraggeber weiter.

§ 4 Vertragsdauer

1. Der Vertrag

   beginnt am .....

   und endet

   - am .....
   - mit Auftragserledigung

   und wird auf unbestimmte Zeit geschlossen.

   Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.

2. Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrags berechtigt, wenn der Auftragnehmer trotz schriftlicher Aufforderung die vereinbarten Leistungen nach § 1 nicht ordnungsgemäß erbringt oder seine Pflichten nach § 3 verletzt.

§ 5 Vergütung und Kostenerstattung

Abmachungen über die Vergütung und Zahlungsweise sowie Aufteilung der Kosten zwischen Auftraggeber und Auftragnehmer

§ 6 Haftung

Treten fehlerhafte Arbeiten auf, so kann der Auftraggeber die kostenlose Berichtigung der Arbeiten verlangen. Der Anspruch auf kostenlose Berichtigung setzt voraus, dass der Auftraggeber die fehlerhaften Arbeiten innerhalb von..... Monaten nach Auslieferung schriftlich unter Beifügung der für eine Berichtigung notwendigen Unterlagen beanstandet.

Bei Programmierarbeiten gilt eine Gewährleistungszeit für die Behebung von Programmfehlern von..... Monaten. Danach auftretende Fehler werden im Rahmen der Wartung zu den üblichen Vergütungssätzen behoben.

§ 7 Schadensersatz

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro *(etwa bis 20 Prozent des Auftragswertes)* vereinbart.

§ 8 Nichterfüllung der Leistung

1. Bei Nichterfüllung der Auftragsleistung durch den Auftragnehmer ist der Auftraggeber berechtigt, soweit er nicht von seinem Kündigungsrecht nach § 4 Gebrauch macht, im Benehmen mit dem Auftragnehmer ein anderes Dienstleistungsunternehmen zu beauftragen. Die dabei entstehenden Mehrkosten gehen zu Lasten des Auftragnehmers.
2. Kann der Auftragnehmer die vereinbarte Leistung wegen höherer Gewalt, Krieg, Aufruhr, Streik, Aussperrung oder Stromausfall nicht rechtzeitig erfüllen, so ist er von der Leistung frei. Die Beweislast hierfür obliegt jedoch dem Auftragnehmer. Der Auftraggeber hat in diesem Falle keinen Anspruch auf Schadenersatz. Er hat jedoch das Recht, ein anderes Dienstleistungsunternehmen mit der Auftragsausführung zu beauftragen.

§ 9 Sonstiges

1. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Alle Kundendaten sind in diesem Zusammenhang rechtzeitig vor Eintritt dieser Maßnahmen von den betroffenen DV-Komponenten zu entfernen.
2. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
3. Sonstige wichtige aufgabenspezifische Regularien:
   .....
4. Ansprechpartner des Auftraggebers sind:

   .....
   (Name, Funktion, Erreichbarkeit)

   Ansprechpartner beim Auftragnehmer sind:

   .....
   (Name, Funktion, Erreichbarkeit)

   Bei einem Wechsel oder einer längerfristigen Verhinderung eines Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

5. Änderungen und Ergänzungen dieses Vertrages bedürfen einer schriftlichen Vereinbarung.

§ 10 Gerichtsstand und Schlussbestimmungen

(Vertragsspezifische Besonderheiten; Gerichtsstand)

_____ _____

(Ort, Datum) (Unterschrift Auftraggeber)

_____ _____

(Ort, Datum) (Unterschrift Auftragnehmer)

Aufstellung der Maßnahmen zum Datenschutz

Patienteninformation zum Datenschutz in der Praxis

Auftragsverarbeitung: Zusammenarbeit mit Dienstleistern

Die Praxissoftware wird gewartet, Akten- und Datenträger müssen nach Ablauf der Aufbewahrungsfrist vernichtet werden. Immer dann, wenn ein externer Dienstleister auf Patienten- oder Mitarbeiterdaten zugreifen kann, ist der Abschluss eines Vertrages zur Auftragsverarbeitung (als Anlage zum Hauptvertrag) erforderlich.

Die Auftraggeber müssen sich ferner davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollen dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

Auftragsverarbeitung: ja oder nein?

Eine Auftragsverarbeitung liegt nicht nur bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung vor. Weitere Beispiele sind die Nutzung von Cloud-Systemen und die Terminvergabe durch Externe (die Terminservicestellen der KVen fallen nicht darunter).

Dagegen ist eine rein technische Wartung der IT-Infrastruktur durch einen Externen, zum Beispiel Arbeiten an der Stromzufuhr, Kühlung oder Heizung, keine Auftragsverarbeitung.

Dies gilt ebenso bei der Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörigen anderer Berufe, die als „Geheimnisträger" gelten. Auch hier liegt in der Regel keine Auftragsverarbeitung vor.

Das ist zu tun

Schritt 1: Schauen Sie zunächst, ob Sie für Ihre Dienstleistungsverträge (z.B. zur Wartung der Praxis-EDV) jeweils einen Vertrag zur Auftragsverarbeitung haben, und passen Sie diesen in Abstimmung mit dem Auftragnehmer gegebenenfalls an.

Schritt 2: Ist das nicht der Fall, sprechen Sie Ihren Dienstleister an. Er benötigt einen Vertrag zur Auftragsverarbeitung und wird Ihnen in der Regel einen Entwurf zusenden.

Folgende Inhalte sollte der Vertrag enthalten:

- Gegenstand und Dauer der Verarbeitung (um welche Leistung handelt es sich, wie lange wird diese beauftragt)
- Art und Zweck der Verarbeitung (wozu dient sie, welches Ziel soll erreicht werden)
- Art der personenbezogenen Daten und Kategorien betroffener Personen (z.B. Zugriff auf Gesundheitsdaten)
- Rechte und Pflichten des Auftraggebers sowie dessen Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung berechtigten Personen zur Vertraulichkeit
- Benennung der technischen und organisatorischen Maßnahmen, die das

Unternehmen zum Schutz personenbezogener Daten durchführt (z.B. Einhaltung von Vorgaben der ISO/IEC 27001)

Verpflichtung des Auftragnehmers zur Unterstützung des Auftraggebers bei:

Anfragen und Ansprüchen Betroffener im Zusammenhang mit der Auftragsverarbeitung

der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung

Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung

Verpflichtung des Auftragnehmers, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten bereitzustellen. Möglich ist auch eine Überprüfung oder Inspektion durch einen vereinbarten Prüfer.

Schritt 3: Lassen Sie sich vom Dienstleister ein geeignetes Zertifikat, zum Beispiel ISO/IEC 27001, vorlegen. Das Zertifikat dient dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der Daten beim Auftragnehmer. Eine weitergehende Pflicht zur Kontrolle durch Sie besteht nicht.

Große Praxen und große MVZ

Datenschutzbeauftragten benennen – ab zehn Personen

Darüber hinaus kann dies erforderlich sein

Datenschutz-Folgenabschätzung

Einwilligungserklärungen anpassen

Datenschutzerklärung auf der Internetseite