ADV-Vertrag für das Gesundheitswesen

Eine Zusammenarbeit von

Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Arbeitskreis „Medizin“

Bundesverband Gesundheits-IT e. V.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Die Autoren sind keine Juristen. Insofern können und dürfen sie keine rechtsverbindlichen Auskünfte geben. Daher ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen. Eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen für das jeweilige Krankenhaus und die jeweilige Situation anhand der für dieses Krankenhaus geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Grafiken, Tondokumente, Videosequenzen und Texte zu beachten, von ihnen selbst erstellte Grafiken, Tondokumente, Videosequenzen und Texte zu nutzen oder auf lizenzfreie Grafiken, Tondokumente, Videosequenzen und Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Stand der Bearbeitung ist 10. Dezember 2014.

Copyright

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

1. Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:
http://creativecommons.org/licenses/by/4.0/deed.de

Inhaltsverzeichnis

1. Vorwort

Warum noch eine Vorlage für einen ADV-Vertrag, wo es doch von den verschiedensten Institutionen und Organisationen schon Vorlagen für einen ADV-Vertrag gibt? Weil keine dieser Vorlagen auf die Besonderheiten im Gesundheitswesen eingeht, also auf die Belange, die beispielsweise für eine Arztpraxis oder ein Krankenhaus relevant sind.

Die bisher vorliegenden Vorlagen für einen ADV-Vertrag gehen auf die Anforderungen des Bundesdatenschutzgesetzes ein: Jedoch unterliegt das Gesundheitswesen dem Föderalismus und somit gelten in jedem Bundesland eigene Datenschutzbestimmungen bezüglich der Patientendaten in einem Krankenhaus. Zudem existieren noch evangelische und katholische Datenschutzgesetze, die ebenfalls beachtet werden müssen. Dazu kommen noch datenschutzrechtliche Regelungen, die in diversen Gesetzen verstreut sind wie beispielsweise:

- Gesetze/Verordnungen bezüglich Arzneimitteln bzw. deren Verabreichung
- Infektionsmeldegesetze
- Krebsregistergesetze
- Sozialgesetzbücher
- Berufsordnungen der jeweiligen Landesärztekammern
- die Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen
- ...

Besonderheiten des Gesundheitswesens

In einer ADV-Vertragsvorlage für das Gesundheitswesen darf man erwarten, dass man Auslegungen und ggfs. Regelungen zu Themen wie

- Regelung bzgl. Umgang mit Zurückbehaltungsrecht i. S. v. §273 BGB
- Schadensersatz- und Haftungsfragen
- Umgang mit den Informationspflichten
- Regelungen zu Wünschen bzgl. einer Zweckänderung durch den Auftragnehmer, z. B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung
- Fragen zu Sozialdaten
- Behandlung der sich aus §203 StGB ergebenden Fragen sowie dem Umgang hinsichtlich Beschlagnahmeschutz
- Umgang mit Datenverarbeitung außerhalb EU/EWR, d. h. auch Umgang mit EU-Standardvertragsklausen

findet. Die immer stärker werdende Vernetzung im Gesundheitswesen und der damit auftauchende verstärkte Einsatz von Gesundheitsportalen – egal ob man sie jetzt elektronische Fallakte, elektronische Patientenakte nennt – erfordert zusätzlich die Betrachtung von Anforderungen aus dem TKG und dem TMG, d. h. Themen wie

- Verpflichtung entsprechend TKG/UWG
- Informationspflichten gemäß §13 TMG

müssen also gleichfalls bedacht werden.

Bildung einer Arbeitsgruppe

Diese Vielzahl von Gründen führte dazu, dass man sich durch die Gründung einer Arbeitsgruppe bestehend aus Vertretern der Verbände

- Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (BvD)
- Bundesverband Gesundheits-IT e. V. (bvitg)
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)

des Themas annahm und einen kommentierten Muster-ADV-Vertrag erstellte. Allen Beteiligten war bewusst, dass es nicht „den" ADV-Vertrag geben kann, sondern dass ein ADV-Vertrag die individuellen Anforderungen widerspiegeln muss. Daher finden sich für verschiedene Anforderungen optionale Ergänzungen oder auch alternative Formulierungen im Text. Alternative Textpassagen werden durch die Abkürzung „Alt.", optionale Textteile durch die Abkürzung „Opt." hervorgehoben.

Ergebnis

Diese Ausarbeitung orientierte sich bei der Erstellung an der „Mustervertragsanlage zur Auftragsdatenverarbeitung" in der Version 3.0 vom BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), die Stand heute unter http://www.bitkom.org/de/themen/50792_45940.aspx verfügbar ist. Allerdings wurden die aus Sicht der Autoren dieser Ausarbeitung zusammengehörenden Punkte gemeinsam dargestellt, was im Vergleich zum BITKOM-Entwurf zu einer anderen Strukturierung führte. Ergänzend erfolgte eine aus Sicht der Autoren erforderliche Darstellung von ergänzenden Themenpunkten aus der Perspektive des Gesundheitsdatenschutzes. Genauer gesagt: Durch die Vertreter von BvD und GDD flossen die Anforderungen der Datenschutzbeauftragten der Auftraggeber (Krankenhäuser), durch den bvitg die Sichtweise der Auftragnehmer (IT-Hersteller) und durch die GMDS auch die Anforderungen aus Forschung und Lehre ein. Weitere Organisationen und Verbände unterstützten die Arbeitsgruppe durch ihre Kommentierungen.

Dabei wird an vielen Stellen auf die Besonderheiten beim Umgang mit Patientendaten in Krankenhäusern eingegangen, da hier spezialgesetzliche Vorgaben existieren. Auch wenn diese Gesetze für Arztpraxen, Pflegeheime usw. diese Gesetze nicht gelten, so wurde bei der Erstellung dieser Ausarbeitung darauf geachtet, dass die in diesem Muster-ADV-Vertrag enthaltenen Formulierungen auch innerhalb anderer Bereiche des Gesundheitswesens angewendet werden können; die vertraglichen Bestandteile, welche ein ADV-Vertrag abdecken muss, sind von der Grundstruktur für Arztpraxis, Krankenhaus, Pflegeheim, Rehabilitationseinrichtung und andere Einrichtungen des Gesundheitswesens identisch.

Im Abschnitt bzgl. des Vertragstextes wird häufiger auf Regelungen des Bundesdatenschutzgesetzes (BDSG) verwiesen. Für die meisten Krankenhäuser gelten andere datenschutzrechtliche Gesetze, jedoch entsprechen die inhaltlichen Anforderungen an einen ADV-Vertrag aus den Landesdatenschutzgesetzen, kirchlichen Bestimmungen sowie den Sozialgesetzbüchern denen, die im BDSG formuliert wurden. Zur besseren Lesbarkeit wurde daher darauf verzichtet, neben den Paragraphen des BDSG auch noch an allen Stellen die Paragraphen der anderen gesetzlichen Bestimmungen aufzuzählen. Insbesondere unter der Berücksichtigung, dass im ADV-Vertrag zwischen Auftraggeber und Auftragnehmer Regelungen vereinbart werden, ist es im ADV-Vertrag ausschließlich von Belang, dass die für den Auftragnehmer geltenden rechtlichen Anforderungen an eine Auftragsdatenverarbeitung abgebildet werden.

Sicher löst ein ADV-Vertrag nicht das Problem, dass für Daten, die dem §203 StGB unterliegen, eine spezialgesetzliche Offenbarungsbefugnis erforderlich ist. Hier wünscht man sich vom Gesetzgeber bessere bzw. einheitliche Lösungen. Die Arbeitsgruppe möchte jedoch mit diesem Muster-ADV-Vertrag eine Hilfestellung geben, das Thema im Gesundheitswesen so weit wie möglich praxisgerecht für Auftragnehmer (IT-Hersteller) und Auftraggeber (Krankenhäuser) vertraglich umsetzen zu können. Anregungen zu unserem Muster nehmen wir gerne entgegen.

2. Allgemeines

Eine Auftragsdatenverarbeitung (ADV) findet sehr häufig statt. Allerdings wurde festgestellt, dass meist die rechtlichen Voraussetzungen für eine Auftragsdatenverarbeitung nicht oder nicht vollständig eingehalten werden[1]. Die Auftragsdatenverarbeitung ist eine „privilegierte“ Form der Funktionsübertragung, für die der Gesetzgeber vertragsrechtliche Anforderungen (§11 BDSG, §80 SGB X, kirchliche sowie landesrechtliche Regelungen) stellt. Aufgrund der gesetzlich vorgeschriebenen vertragsrechtlichen Gestaltung bleibt der Auftraggeber datenschutzrechtlich verantwortlich. Als "privilegiert" wird diese Form der externen Datenverarbeitung deswegen angesehen, weil es sich hierbei nicht um eine datenschutzrechtliche Übermittlung der Daten handelt. Damit wird keine gesetzliche Erlaubnis zur Weitergabe der Daten an einen externen Dienstleister (Auftragnehmer) benötigt bzw. muss keine Abwägung bspw. gemäß §28 Abs. 6 und 7 BDSG vorgenommen werden, die bei Gesundheitsdaten immer zugunsten des Betroffenen ausgelegt werden müsste. Eine Einverständniserklärung des jeweiligen Patienten (Betroffenen) ist ebenfalls nicht erforderlich. Dies gilt nicht vor dem Hintergrund des §203 StGB, sodass dem Auftraggeber eine Befugnis zum Offenbaren vorliegen muss. Eine rein formale Lösungsmöglichkeit wäre neben anderen technischen oder organisatorischen Maßnahmen, eine Schweigepflichtentbindung, welche in der vorliegenden Form so faktisch nicht umgesetzt werden kann.

Eine Auftragsdatenverarbeitung kann daher nur stattfinden, wenn der Auftragnehmer ausschließlich auf Anweisung des Auftraggebers tätig wird und der Auftraggeber die Art und Weise festlegt, in welcher der Auftragnehmer die Daten bearbeitet. Typische Erkennungsmerkmale für Auftragsdatenverarbeitung sind:

- Es fehlt eine Entscheidungsbefugnis des Auftragnehmers.
- Es wurde vertraglich ausgeschlossen, dass der Auftragnehmer Daten zu eignen Zwecken verarbeitet oder nutzt.
- Der Auftragnehmer ist weisungsgebunden bezüglich der Datenverarbeitung.
- Es dürfen nur Daten verarbeitet werden, die der Auftraggeber zur Verfügung stellt, es sei denn, der Auftrag umfasst auch die Erhebung von personenbezogenen Daten.
- Es existiert keine (vertragliche) Beziehung des Auftragnehmers zu den Betroffenen.
- Der Auftragnehmer tritt (gegenüber den Betroffenen) nicht mit dem eigenen Namen auf.

Ein Vertrag über eine Auftragsdatenverarbeitung kann entweder als Anlage zu einem Hauptvertrag oder als Einzelvertrag für sich stehen.

Nachfolgend einige typische Beispiele für eine Auftragsdatenverarbeitung durch externe Dienstleister:

- Auslagerung von IT-Systemen und oder Daten in ein externes Rechenzentrum (Outsourcing)
- Papier-/Aktenvernichtung sowie die Vernichtung von Datenträgern
- Archivierungsdienstleistungen
- Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene oder personenbeziehbare Daten nicht ausgeschlossen werden kann.

[1] Hansen-Oest S. Auftragsdatenverarbeitung. online, verfügbar unter http://www.datenschutz-guru.de/auftragsdatenverarbeitung/

Basierend auf dem Grundsatz von Treu und Glauben (§242 BGB) haben die Parteien alles zu unterlassen, was den Vertragszweck und den Leistungserfolg beeinträchtigen oder gefährden könnte. Daraus ergeben sich insbesondere Obliegenheiten und Pflichten zur Mitwirkung und gegenseitigen Information, sodass sowohl Auftragnehmer wie auch Auftraggeber dafür Sorge tragen müssen, dass ein ADV-Vertrag abgeschlossen wird, wenn eine Auftragsdatenverarbeitung vorliegt.

2.1 Lohnt sich die Ausarbeitung, da doch bald die europäische Datenschutz-Grundverordnung verabschiedet wird?

Aus Medien wie Nachrichtenzeitschriften und dem Fernsehen ist bekannt, dass die Europäische Union an einer Datenschutz-Grundverordnung (DS-GVO) arbeitet[2], die - wenn sie denn verabschiedet wird - letztlich vorrangig gegenüber den deutschen Gesetzen gelten wird. D. h. Bestimmungen bzgl. der ADV sind entsprechend dieser Grundverordnung umzusetzen und es stellt sich die Frage, ob mit dieser Grundverordnung die vorliegende Ausarbeitung Ihren Zweck noch erfüllt.

Auch die geplante DS-GVO regelt in dem Kapitel IV „Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter“ in den Artikeln 22 bis 32 die Verarbeitung personenbezogener Daten im Auftrag. Nimmt man den zum Zeitpunkt der Ausarbeitung vorhandenen Entwurf der DS-GVO, so sieht man, dass die Artikel 22 bis 32 nahezu identische Anforderungen an die Auftragsdatenverarbeitung stellen wie die heutige deutsche Gesetzgebung. Innerhalb Deutschlands wird sich nach heutiger Erkenntnis daher bzgl. des Vorgehens bei der Auftragsdatenverarbeitung mit der geplanten DS-GVO nicht viel ändern, insbesondere behalten die Anforderungen an den ADV-Vertrag ihre Gültigkeit.

3. Abgrenzung

Diese Ausarbeitung befasst sich ausschließlich mit Anforderungen aus *Datenschutzgesetzen* bzgl. der Nutzung von personenbezogenen Patientendaten im Bereich des Outsourcings im Gesundheitswesen. Nicht Bestandteil dieser Ausarbeitung sind andere Anforderungen an Outsourcing-Vorhaben, seien sie rechtlicher Natur oder Empfehlungen der entsprechenden Fachorgane. Hier wird auf die gängige Literatur verwiesen. Insbesondere kann Stand heute mit den Regelungen der Auftragsverarbeitung nicht die Fragestellung bzgl. einer daraus resultierenden Offenbarungsbefugnis gemäß §203 StGB für ganz Deutschland abgeleitet werden. Der durch die geltende Gesetzgebung entstehende Widerspruch, dass eine Arztpraxis oder ein Krankenhaus ein datenschutzrechtlich konform geregeltes Outsourcing von Leistungen betreiben, zugleich aber eventuell gegen geltendes Strafrecht verstoßen kann, ist daher auch durch einen ADV-Vertrag nicht aufzulösen. (Für weitere Details siehe auch die Kommentierung der Präambel zum Mustervertrag unten.)

4. Wartung / Fernwartung

Bei der Wartung von Datenverarbeitungsanlagen, insbesondere von medizinischen Informationssystemen oder Medizingeräten durch den Hersteller, kann der Auftraggeber

[2] Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). [Online, zitiert am 2014-11-01]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

nicht die Art und Weise bestimmen, in welcher der Auftragnehmer vorgehen muss. Der Auftragnehmer, der in der Regel auch Hersteller der Datenverarbeitungsanlage ist, ist als Einziger in der Lage zu bestimmen, welche Maßnahmen für den ordnungsgemäßen Betrieb der Anlage erforderlich sind oder welche Maßnahmen im Fehlerfall getroffen werden müssen. Damit verliert der Auftraggeber einen Teil seiner Kontrollmöglichkeit bzgl. der Verwendung seiner Daten, was vielleicht für eine Funktionsübertragung sprechen würde.

Jedoch muss man festhalten, dass Wartung und Fehlerbeseitigung von medizinischen Datenverarbeitungsanlagen in erster Linie nicht die gespeicherten Daten betreffen, sondern die Software, mit welcher die Daten verarbeitet werden. Nur in begründbaren Ausnahmefällen muss der Auftragnehmer auf personenbezogene oder personenbeziehbare Daten zurückgreifen. Daher hat der Gesetzgeber die Prüfung und Wartung automatisierter Verfahren der Datenverarbeitung bzw. von Datenverarbeitungsanlagen ausdrücklich in die Auftragsdatenverarbeitung einbezogen.

Generell muss der Vertrag zwischen Auftragnehmer und Auftraggeber auch die Interessen der betroffenen Patienten gebührend berücksichtigen, damit hier kein Vertrag zu Lasten Dritter abgeschlossen wird und durch einen nicht normkonformen Vertrag die Privatautonomie der Patienten beeinträchtigt wird. Dies könnte letztlich zivilrechtliche Ansprüche der betroffenen Patienten gegenüber dem Auftraggeber beinhalten. Weiterhin können aus einer unbefugten Offenbarung entsprechend §203 StGB strafrechtliche Konsequenzen folgen. Daher ist es gerade im Bereich der Wartung von informationstechnischen Systemen durch Hersteller, die als Auftragnehmer gegenüber dem Auftraggeber eine Wissenshoheit bzgl. der Systeme besitzen, wichtig, dass der Auftraggeber in der vertraglichen Gestaltung der Auftragsdatenverarbeitung darauf achtet, dass er erkennbar der „Herr der Daten“ bleibt. Ansonsten ist von einer Funktionsübertragung auszugehen und der Auftraggeber benötigt die Einwilligung aller Betroffenen, damit der Auftragnehmer im Rahmen der geplanten Wartung/Fernwartung tätig werden darf.

5. Sozialdatenschutz vs. Krankenhaus/Arztpraxis

Zur Wahrung des Sozialgeheimnisses gemäß §35 SGB I sind die Leistungsträger entsprechend §12 in Verbindung mit §§18 bis 29 SGB I verpflichtet, sofern Sozialdaten erhoben, verarbeitet oder genutzt werden. In §67 Abs. 1 SGB X erfolgt die Legaldefinition von Sozialdaten. Demnach sind Sozialdaten alle „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in §35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden“. Zu den in §35 SGB I genannten Stellen gehören alle in §§18-29 SGB I genannten öffentlichen Vereinigungen, Integrationsfachdienste, die Künstlersozialkasse, die Deutsche Post AG, Behörden der Zollverwaltung, Versicherungsämter, Gemeindebehörden, anerkannte Adoptionsvermittlungsstellen nach §2 Abs. 2 des Adoptionsvermittlungsgesetzes sowie die Stellen, welche Aufgaben nach §67c Abs. 3 SGB X wahrnehmen.

Es kann daher nicht gesagt werden, dass ein Leistungserbringer im Gesundheitswesen (Arztpraxis oder Krankenhaus) grundsätzlich dem Sozialdatenschutz unterliegt[3]. Vielmehr muss festgehalten werden, dass Stätten der Leistungserbringung wie Krankenhäuser,

[3] Dies ist auch aus dem Urteil des Bundessozialgerichtes (Urteil vom 23. 7. 2002 - B 3 KR 64/01 R) ableitbar, nachdem eine Krankenkasse kein eigenständiges Recht auf Einsichtnahme in die Behandlungsunterlagen hat; wären es Sozialdaten der Krankenkasse, so hätte die Krankenkasse selbstverständlich ein Anrecht auf Einsichtnahme

Arztpraxen, Pflegeheime usw. keine Normadressaten im Sinne des Sozialdatenschutzes sind. Im Sozialrecht gibt es eine Vielzahl von Vorschriften bzgl. der Erhebung, Verarbeitung und Nutzung von Patientendaten durch ein Krankenhaus. Entsprechend §67a Abs. 2 können Sozialdaten direkt beim Leistungserbringer, also auch im Krankenhaus erhoben werden. Damit könnte argumentiert werden, dass Krankenhäuser Sozialdaten für die Krankenkasse erheben. Aus §67c SGB X in Verbindung mit §284 SGB V kann abgeleitet werden, dass beim Leistungserbringer gespeicherte Patientendaten zugleich gespeicherte Sozialdaten darstellen.

Folgt man dieser Argumentation, muss festgehalten werden, dass die Anforderungen zur Auftragsdatenverarbeitung aus §80 SGB X auch für Krankenhäuser gelten. D. h. die bundesrechtlichen Anforderungen zur ADV-Vertragsgestaltung sind von allen Leistungserbringern – Arztpraxen wie auch Krankenhäusern – in den jeweils von ihnen abgeschlossenen Verträgen abzubilden.

Es ist die Ansicht der Autoren dieser Ausarbeitung, dass die Argumentation falsch ist. Nach Ansicht der Arbeitsgruppe sind die Daten bei Leistungserbringern wie einer Arztpraxis oder einem Krankenhaus keine Sozialdaten, da die Erhebung und Verarbeitung zunächst dem Zweck der Behandlung und ordnungsgemäßen Dokumentation dient. Erst durch die Datenübermittlung an den Leistungsträger (z. B. Krankenkasse zum Zweck der Abrechnung) werden die Behandlungsdaten dort zu Sozialdaten. Da jedoch keine abschließende Rechtsprechung zu diesem Thema verfügbar ist, muss sich hierzu jeder eine eigene Rechtsmeinung bilden und ggfs. auch vertreten.

6. Schweigepflicht gemäß §203 StGB und Auftragsdatenverarbeitung

Die Verpflichtung zur Einhaltung einer ärztlichen Schweigepflicht ist sowohl im Strafgesetzbuch (§203 StGB) als auch in den Berufsordnungen der Landesärztekammern (§9 BO) festgelegt. Der strafrechtlichen Schweigepflicht unterliegen auch die bei einem Arzt berufsmäßig tätigen Gehilfen und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen.

Der geschützte Geheimbereich ist weit zu ziehen: zum geschützten Bereich gehören sowohl die Tatsachen und Umstände, die sich auf den Gesundheitszustand des Patienten selbst beziehen als auch alle Gedanken, Meinungen, Empfindungen, Handlungen, familiären, finanziellen und beruflichen Verhältnisse, an deren Geheimhaltung der Patient oder ein Dritter, auf den sich das Geheimnis bezieht, erkennbar ein Interesse hat[4]. Selbst die Tatsache, dass sich ein Patient überhaupt in ärztlicher Behandlung befindet oder befunden hat, zählt - ebenso wie der Name des Patienten - zu dem vom Gesetz geschützten Geheimbereich4. Die gesetzliche Schweigepflicht gilt auch über den Tod des Betroffenen hinaus.

Die Vergabe von Auftragsdatenverarbeitung-Vorgängen von Arztpraxen, Krankenhäusern oder Klinikkonzernen wird durch §203 StGB limitiert[5]. Der Gesetzestext dieses Paragrafen steht einer Datenbe- oder verarbeitung bzw. einer Übermittlung von Privatgeheimnissen

[4] Ärztekammer Berlin. (2008) Merkblatt Schweigepflicht. . Online, zitiert am 2014-10-03]; Verfügbar unter http://www.aerztekammer-berlin.de/10arzt/30_Berufsrecht/08_Berufsrechtliches/06_Behandlung_von_Patienten_Pflichten_Empfehlungen/35_Merkblatt_Schweigepflicht.pdf

[5] Parzeller, Markus; Wenk, Maren; Rothschild, Markus A. (2005) Zertifizierte Medizinische Fortbildung: Die ärztliche Schweigepflicht. Dtsch Arztebl; 102(5): A-289 / B-237 / C-224 (Online, verfügbar unter https://www.aerzteblatt.de/pdf.asp?id=45243)

durch bzw. an externe Dienstleister entgegen, selbst wenn es sich hierbei um eine konzerninterne Service- oder IT-Tochtergesellschaft handelt, denn bei der Auftragsdatenverarbeitung erfolgt häufig eine Offenbarung von Patientengeheimnissen an externe Dienstleister, welche dem Gesetzestext des §203 StGB zufolge wahrscheinlich unbefugt erfolgt: Das ärztliche Personal begeht damit strafrechtlich einen Gesetzesverstoß.

Allerdings wird entsprechend §205 Abs. 1 StGB ein Verstoß gegen §203 StGB nur auf Antrag verfolgt, wobei entsprechend §77 Abs. 1 StGB nur

- der Verletzte (= der betroffene Patient)
- bzw. im Falle, dass der Antragsberechtigte geschäftsunfähig oder beschränkt geschäftsfähig ist, der gesetzliche Vertreter
- oder - nach dem Tod des Verletzten - der Erbe

zu einem Antrag auf Strafverfolgung berechtigt ist.

6.1 Offenbarung im Sinne §203 StGB

Der Tatbestand des §203 StGB setzt voraus, dass einer der in Abs. 1 genannten Geheimnisverpflichteten ein fremdes Geheimnis, welches ihm anvertraut worden ist, unbefugt offenbart. Schutzzweck der Vorschrift ist vorrangig die Geheimsphäre des Einzelnen, daneben auch das Allgemeininteresse an der Verschwiegenheit einzelner Berufsgruppen7. Ein Offenbaren im Sinne des §203 StGB ist demnach zunächst jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten[6].

Der Vorschrift liegt die Vorstellung zugrunde, dass nur der Geheimnisverpflichtete mit den Geheimnissen in Berührung kommen muss. Wenn ein Patient oder Mandant seinen Arzt oder Anwalt aufsucht, geht §203 StGB somit davon aus, dass lediglich dieser einen Einblick in den persönlichen Lebensbereich bekommen soll[7]. Dem Wortlaut nach würde bereits die Weitergabe der Geheimnisse an das Pflegepersonal oder Sprechstundenhilfe eine Offenbarung bedeuten. Da dies jedoch jeglichen Funktionsablauf in einer Arztpraxis oder einem Krankenhaus zum Erliegen bringen würde, entspricht es herrschender Ansicht, dass es möglich ist, derartige Hilfskräfte einzuschalten, ohne dass ein Offenbaren im Sinne des §203 StGB vorliegt. Begründet wird dies mit §203 Abs. 3 S. 2 StGB, der auch diejenigen zur Verschwiegenheit verpflichtet, die den Schweigepflichtigen in Bezug auf dessen berufliche Tätigkeit unterstützen. Eine Weitergabe an einen solchen Dritten kann nach einhelliger Ansicht grundsätzlich straflos erfolgen.

Ein Offenbaren liegt ebenfalls dann nicht vor, wenn der Empfänger des Geheimnisses „zum Kreis der zum Wissen Berufenen" gehört, beispielsweise wenn ein weiterer Arzt (Radiologe, Labormediziner, …) im Behandlungsprozess des Patienten integriert ist.

Werden im Rahmen eines Outsourcings hingegen „externe" Dienstleister mit diesen Aufgaben betraut, so werden die Geheimnisse nicht an interne Mitarbeiter weitergegeben, sondern über die Grenzen von juristischen Personen hinweg ausgetauscht. Unklar ist derzeit, inwieweit diese zum Kreis der Gehilfen im Sinne des §203 StGB gezählt werden dürfen.

[6] Ehrmann, Outsourcing von medizinischen Daten – strafrechtlich betrachtet-, 2008,S. 60

[7] Bräutigam P. (2011) §203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416

6.2 Offenbarung und Auftragsdatenverarbeitung

Die Regelungen zur Auftragsdatenverarbeitung entsprechend §11 BDSG begründen keine Offenbarungsbefugnis im Sinne des §203 StGB[8]. Vielmehr wird hier beschrieben, dass der Datenfluss zwischen Auftragnehmer und Auftraggeber rechtlich nicht als Datenübermittlung, sondern als sonstige Art der Datenweitergabe (Datennutzung) angesehen wird: „Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen“ (§3 Abs. 3 Satz 3 BDSG). §1 Abs. 3 S. 2 BDSG stellt klar:
„Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt“. Daher können die Regelungen des BDSG nicht als Erlaubnisnorm gewertet werden.
Eine Offenbarung im Sinne des §203 StGB liegt nicht vor, wenn:

a) Jede Zugriffsmöglichkeit des beauftragten Dritten auf die Patientendaten ausgeschlossen wird. Beispiele:
   - Wartungsarbeiten an Praxisrechnern durch externe Mitarbeiter sind dadurch möglich, dass von einem Geheimnisträger (oder dessen Gehilfen entsprechend §203 StGB) die Arbeiten überwacht werden und dieser darauf achtet, dass kein Zugriff auf Patientendaten erfolgt.
   - Bei einer externen Entsorgung ist ein beaufsichtigendes Begleiten von Transport und Vernichtung möglich.

b) Die Daten vor ihrer Bearbeitung durch externe Mitarbeiterinnen/Mitarbeiter durch den Geheimnisträger oder dessen Gehilfen anonymisiert oder pseudonymisiert werden.

c) Eine weitere Möglichkeit zur Verhinderung einer unzulässigen Offenbarung könnte darin bestehen, dass der Auftragnehmer nicht als externer Dritter angesehen wird, sondern als Gehilfe. In der Offenbarung an einen Berufsgehilfen liegt keine Verletzung der ärztlichen Schweigepflicht nach §203 StGB. Auch bei dem Berufsgehilfen des Arztes ist das Zeugnisverweigerungsrecht des Arztes (§53 StPO) und der Beschlagnahmeschutz für ärztliche Unterlagen (§97 StPO) gewährleistet. Entsprechendes gilt für das zivilrechtliche Zeugnisverweigerungsrecht (§383 Abs. 1 Nr. 6 ZPO).

Die Bestimmungen von bereichsspezifischen Gesetzen, die explizit die Auftragsdatenverarbeitung von im Krankenhaus anfallenden Daten – Patientendaten eingeschlossen – regeln, wie beispielsweise §7 GDSG NRW sind hingegen anders zu bewerten. Aufgrund der Tatsache, dass hier explizite Bestimmungen zur Auftragsdatenverarbeitung von Patientendaten getroffen werden, werden diese Bestimmungen von diversen Autoren als spezial-gesetzgeberische Offenbarungsbefugnis entsprechend §203 StGB angesehen.

[8] Tröndle/Fischer, 50 Aufl. 2001, § 203 StGB, Rd.-Nr. 28, Auernhammer, 3. Aufl. 1993, § 11 BDSG, Rd.-Nr. 10; Gola/Schomerus, 6. Aufl. 1997, § 11 BDSG, Tz. 1.1; Walz in: Simitis/Dammann, § 11 BDSG, Rd.-Nr. 32 f.; Hamburgischer Datenschutzbeauftragter, 16. Tb. 1997, Tz. 18.1.1

6.3 Gehilfe im Sinne von §203 StGB

Voraussetzung für die Annahme eines Gehilfenstatus ist, dass der Schweigepflichtige in seiner Funktion nach §203 StGB unmittelbar unterstützt wird[9]. Die Qualifikation des Tätigwerdenden ist dabei richtigerweise nicht maßgeblich. Erfasst werden nicht nur einfache Hilfstätigkeiten, sondern ein Gehilfe i. S. v. §203 StGB kann auch jemand sein, der hoch qualifizierte Tätigkeiten erbringt[10]. Insofern ist der Begriff Gehilfe nicht mit dem allgemeinen Sprachgebrauch zu erklären.

Der Gehilfe muss nicht zwingend eine der Aufgaben erledigen, die als spezifische Hauptaufgaben des Schweigepflichtigen bezeichnet werden können, also beispielsweise bei einem Arzt die Behandlung und Untersuchung des Patienten. Ausreichend ist auch das Erledigen von Nebenaufgaben, zu denen der Schweigepflichtige verpflichtet ist, beispielsweise das Ausstellen von Rechnungen oder das Verarbeiten von Daten. Zu fordern ist aber, dass die Aufgaben unmittelbar der Berufsausübung dienen und hinreichend eingebunden in die Vertrauensbeziehung zwischen Schweigepflichtigen und Geheimnisträger erfolgen.

Der Schweigepflichtige muss gegenüber dem Gehilfen weisungsberechtigt sein, denn ohne ein solches Weisungsrecht wäre eine Zuordnung zu einer Funktionseinheit bzw. zum Geheimnisverpflichteten willkürlich und unbeständig[11]. Eine Zuordnung ohne ein tatsächliches Weisungsrecht wäre vor dem Hintergrund des geschützten Rechtsgutes nicht hinnehmbar und würde das Geheimnis vollkommen von der Person des Schweigepflichtigen abkoppeln. Dies entspricht nicht dem Willen des Gesetzgebers, der über die Einschränkung in §203 Abs. 1 StGB aufgrund der enumerativen Aufzählung von Schweigepflichtigen auch der Person des Schweigepflichtigen Bedeutung zumessen wollte.

Ein Weisungsrecht ist aber zutreffend dann entbehrlich, wenn sich die Zuordnung zu einer Funktionseinheit schon erkennbar aus anderen Umständen ergibt. Wird beispielsweise innerhalb eines Krankenhauses ein weiterer Arzt in die Behandlung eingeschaltet, ergibt sich schon aus der Zugehörigkeit zu derselben Organisation eine eindeutige Zuordnung, sodass es nicht auf ein vereinbartes oder tatsächliches Weisungsrecht ankommt. Der Patient kann mit solch einer Einschaltung von Personen aus einem von vornherein abgegrenzten Bereich rechnen. Werden aber Personen außerhalb eines solchen Bereichs herangezogen, wie dies beim Outsourcing der Fall ist, dann kann auf ein tatsächliches Weisungsrecht als weiteres notwendiges Kriterium für eine eindeutige Zuordnung nicht verzichtet werden[12].

Dabei ist es unerheblich, ob die Personen die Tätigkeit nur gelegentlich oder als Haupt- bzw. Nebenberuf ausüben, sofern sie weisungsgebunden in das Vertrauensverhältnis eingebunden sind. Damit wird auch Kongruenz zum Strafprozessrecht erzielt, da §53a StPO nach im Vordringen befindlicher Auffassung derart eingebundene Personen ebenfalls als Gehilfen erfasst und über §97 Abs. 4 StPO Beschlagnahmefreiheit für Gegenstände, die im Gewahrsam der Gehilfen sind, gewährleistet[13]. Werden hingegen Aufgaben von gleichgeordneten Personen selbstständig erfüllt, sind diese als externe Dritte und nicht als Gehilfen zu bezeichnen[14].

---

[9] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 114; Tröndle/Fischer, StGB, § 203 Rn. 21; zu den unterschiedlichen, sachlich sich kaum unterscheidenden Formulierungen vgl. Sieber, in: Handbuch Multimedia Recht, Teil 19 Rn. 488

[10] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 118; Klöcker/Meister, Datenschutz im Krankenhaus, S. 36; OLG Oldenburg NStZ 83, S. 39, das auch die Verwaltungsleitung als Gehilfen ansieht

[11] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 115; Ehmann, CR 91, S. 295

[12] Taupitz, MedR 1993, S. 375

[13] Fritzemeyer, in Söbbing: IT-Outsourcing, S. 755

[14] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 114; Neubeck, in: KMR StPO, § 53a Rn. 2ff

Als Gehilfen sind dabei nach herrschender Meinung solche Personen einzuordnen, deren unterstützende Tätigkeit in einem inneren Zusammenhang mit der besonderen Tätigkeit nach §203 Abs. 1, 3 S 1 StGB steht. Diese Tätigkeit ist durch die Beziehung zur ärztlichen Tätigkeit mit der Kenntnisnahme von Geheimnissen verbunden, Beispiele hierfür sind die Tätigkeiten von Sekretärinnen, Krankenschwestern oder internes EDV-Personal[15][16]. Tätigkeiten, die sich lediglich auf die äußeren Bedingungen der jeweiligen Tätigkeit beziehen (Boten, Reinigungspersonal, Chauffeure usw.) fallen hingegen nicht darunter.

Umstritten ist, wie die gesetzliche Formulierung „berufsmäßig tätigen Gehilfen" bzgl. des Passus „berufsmäßig tätig" auszulegen ist. Der Ausdruck umschreibt, wie zuvor beschrieben, den inneren Zusammenhang zwischen der unterstützenden und der besonderen beruflichen, in diesem Fall also der ärztlichen, Tätigkeit. Dies hat zur Konsequenz, dass der Gehilfe seine Tätigkeit nicht als berufliche Haupterwerbsquelle ausüben muss, sondern auch Nebentätigkeiten und ehrenamtliche Aktivitäten erfasst werden[17]. Durch diese Auslegung wird eine Übereinstimmung zum Gehilfenbegriff in §53a StPO erzielt, welcher sich lediglich allgemein auf „Gehilfen" bezieht.[17]

6.4 Schweigepflichtenbindung

Eine Befugnis zur Offenbarung von §203 StGB stellt eine Schweigepflichtentbindung durch den Betroffenen dar, im Falle der hier beschriebenen Auftragsdatenverarbeitung im Gesundheitswesen also eine Schweigepflichtentbindung durch den Patienten.

Bei einer rechtswirksamen Schweigepflichtentbindung müssen aber einige Punkte beachtet werden. Zu diesen gehören[18]:

- Entbindungen von der Schweigepflicht müssen ggfs. nachgewiesen werden und sind daher vorzugsweise schriftlich einzuholen. Auf jeden Fall sollte das Datum der Schweigepflichtentbindung festgehalten werden.
- Eine Schweigepflichtentbindung muss auf der freien Entscheidung des Patienten bzw. der Patientin beruhen, der bzw. die auf die Folgen einer Verweigerung einer Einwilligung hinzuweisen ist.
- Eine Schweigepflichtentbindung kann mit Wirkung für die Zukunft widerrufen werden.
- Es ist aufzuführen, wer von seiner Schweigepflicht entbunden werden soll. Der Arzt bzw. die Ärzte ist bzw. sind namentlich zu benennen.
- Soweit möglich sind die Daten konkret in der Erklärung zu anzugeben. Ist dies wegen des Umfangs der Unterlagen nicht möglich, so sind diese dennoch präzise abschließend zu beschreiben.
- Der Zweck der Offenbarung muss benannt sein.
- Der Empfänger ist namentlich zu benennen.
- Der Erklärung muss zu entnehmen sein, ob eine einmalige oder wiederkehrende Offenbarung beabsichtigt ist.

[15] Lensdorf L, Mayer-Wegelin C, Mantz R. (2009) Outsourcing unter Wahrung von Privatgeheimnissen - Wie das mögliche Hindernis des § 203 Abs. 1 StGB überwunden werden kann. CR: 62-68

[16] Heghmanns M, Niehaus H. (2008) Outsourcing im Versicherungswesen und der Gehilfenbegriff des §203 III 2 StGB. NStZ: 57ff

[17] Weidemann in Beck'scher Online-Kommentar StGB (2013) Gleichgestellter Täterkreis des § 203 Abs. 3 StGB. Rn 21-24

[18] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Erklärung zur Entbindung von der Schweigepflicht. Online, zitiert am 2014-10-03]; Verfügbar unter https://www.datenschutzzentrum.de/medizin/arztprax/entbind.htm

6.5 Literatur

1) Bräutigam P. (2011) §203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416
2) Bruns W, Andreas M, Debong B. (1999) Ärztliche Schweigepflicht im Krankenhaus. ArztRecht: 32 - 37
3) Buchner B. (2013) Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht. MedR: 337 - 342
4) Conrad I, Fechtner S. (2013) IT-Outsourcing durch Anwaltskanzleien nach der Inkasso-Entscheidung des EuGH und dem BGH, Urteil vom 7.2.2013 - Datenschutzrechtliche Anforderungen. CR: 137-148
5) Frewer A, Säfken C. (2003) Ärztliche Schweigepflicht und die Gefährdung Dritter - Medizinethische und juristische Probleme der neueren Rechtsprechung. Ethik Med: 15 – 24
6) Giesen T. (2012) Zum Begriff des Offenbarens nach §203 StGB im Falle der Einschaltung privatärztlicher Verrechnungsstellen. NStZ: 122ff
7) Heghmanns M, Niehaus H. (2008) Outsourcing im Versicherungswesen und der Gehilfenbegriff des §203 III 2 StGB. NStZ: 57ff
8) Hoenike M, Hülsdunk L. (2004) Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung? MMR:788ff
9) Huffer H. (2002) Schweigepflicht im Umbruch. NJW: 1382-1386
10) Jandt S, Roßnagel A, Wilke D. (2011) Outsourcing der Verarbeitung von Patientendaten - Fragen des Daten- und Geheimnisschutzes. NZS: 641ff
11) Kern BR. (2006) Der postmortale Geheimnisschutz. MedR: 205 - 208
12) Klein H. (2010) Schweigepflicht versus Offenbarungspflicht. RDG: 172ff
13) Klöcker I. (2001) Schweigepflicht des Betriebsarztes im Rahmen arbeitsmedizinischer Vorsorgeuntersuchungen. MedR: 183 - 187
14) Kort M. (2011) Strafbarkeitsrisiken des Datenschutzbeauftragten nach §STGB §203 StGB beim IT-Outsourcing, insbesondere in datenschutzrechtlich „sichere“ Drittstaaten. NstZ: 193 - 195
15) Kroschwald S, Wicker M. (2012) Kanzleien und Praxen in der Cloud – Strafbarkeit nach §203 StGB. CR: 758-764
16) Leisner W. (2010) Einschaltung Privater bei der Leistungsabrechnung in der Gesetzlichen Krankenversicherung - Verfassungsrechtliche Vorgaben für eine anstehende gesetzliche Neuregelung. NZS: 129 -136
17) Lensdorf L, Mayer-Wegelin C, Mantz R. (2009) Outsourcing unter Wahrung von Privatgeheimnissen - Wie das mögliche Hindernis des §203 Abs. 1 StGB überwunden werden kann. CR: 62-68
18) Lewinski K. (2004) Schweigepflicht von Arzt und Apotheker - Datenschutzrecht und aufsichtsrechtliche Kontrolle. MedR: 95-104
19) Menzel HJ. (2013) Auftragsdatenverarbeitung im Sozial- und Gesundheitswesen. RDV: 59 - 66
20) Moderegger C. (2001) Leitfaden zur Telearbeit. ArbRB: 90-92
21) Paul JA, Gendelev B. (2012) Outsourcing von Krankenhausinformationssystemen - Praxishinweise zur rechtskonformen Umsetzung. ZD: 315-321
22) Spickhoff A. (2005) Postmortaler Persönlichkeitsschutz und ärztliche Schweigepflicht. NJW: 1982-1984
23) Szalai S, Kopf R. (2012) Verrat von Mandantengeheimnissen - Ist Outsourcing strafbar nach §203 StGB? ZD: 462-468

24) Ulmer CD. (2012) Datenverarbeitung und Datenschutz im Gesundheitswesen – technische Möglichkeiten und rechtliche Grundlagen. RDG: 272-278
25) Waider, H. (2006) Ärztliche Schweigepflicht im psychiatrischen Krankenhaus. Recht & Psychiatrie 24: 65-74
26) Weichert T. (2004) Die Krux mit der ärztlichen Schweigepflichtentbindung für Versicherungen. NJW: 1695ff
27) Welke WA. (2008) Zulässigkeit von Durchsuchungen in Arztpraxen - Anmerkung zum Beschluss des BVerfG vom 21. 1. 2008 – 2 BvR 1219/07. MedR: 732 - 734
28) Wienke A, Sauerborn J. (2000) EDV-gestützte Patientendokumentation und Datenschutz in der Arztpraxis. MedR: 517-519

6.5 Gerichtsurteile

1) Die versicherungsrechtliche Obliegenheit zur Schweigepflichtentbindung
   Gericht: BVerfG
   Datum: 17.07.2013
   Aktenzeichen: 1 BvR 3167/08
2) Verletzung der ärztlichen Schweigepflicht wegen Verdachts der Kindesmisshandlung
   Gericht: KG
   Datum: 27.06.2013
   Aktenzeichen: 20 U 19/12
3) Keine Schweigepflicht für Inhaber von Zahnlaboren
   Gericht: OLG Köln
   Datum: 19.09.2011
   Aktenzeichen: 5 U 42/11
4) Verletzung des allgemeinen Persönlichkeitsrechts des Patienten durch Attest eines beamteten Chefarztes
   Gericht: OLG München
   Datum: 04.02.2010
   Aktenzeichen: 1 U 4650/08
5) Kein Ordnungsgeld gegen Zeugen bei Berufung auf Zeugnisverweigerungsrecht
   Gericht: OLG Düsseldorf
   Datum: 04.12.2009
   Aktenzeichen: 17 W 7/10
6) Zeugnisverweigerungsrecht einer Krankenschwester
   Gericht: OLG Hamm
   Datum: 20.01.2009
   Aktenzeichen: 5 Ws 24/09
7) Die ärztliche Schweigepflicht bezieht sich auch auf die Identität des Patienten
   Gericht: OLG Karlsruhe
   Datum: 11.08.2006
   Aktenzeichen: 14 U 45/04
8) Kein Verstoß gegen die ärztliche Schweigepflicht bei der Vorlage von Patientenunterlagen an die Ärztliche Stelle
   Gericht: VG Frankfurt/Main
   Datum: 13.02.2008
   Aktenzeichen: 4 E 1892/07
9) Grenzen ärztlicher Schweigepflicht; Aufklärung über Aids-Erkrankung des Lebenspartners
   Gericht: OLG Frankfurt

Datum: 08.07.1999
Aktenzeichen: 8 U 67/99

10) Archivierung von Behandlungsunterlagen durch private Unternehmen
Gericht: OLG Düsseldorf
Datum: 20.08.1996
Aktenzeichen: 20 U 139/95

11) Zum Umfang der Schweigepflicht eines im Strafvollzug tätigen Anstalts(zahn)arztes
Gericht: OLG Karlsruhe
Datum: 07.04.1993
Aktenzeichen: 2 Ws 13/93

12) Übergabe der Patienten- und Beratungskartei einer Arztpraxis - Patienteneinwilligung
Gericht: BGH
Datum: 11.12.1991
Aktenzeichen: VIII ZR 4/91

13) Ärztliche Schweigepflichtverletzung: Mitteilung der erhobenen Befunde durch einen konsiliarisch herangezogenen Psychologen an Hausarzt
Gericht: LG München I
Datum: 01.10.1991
Aktenzeichen: 23 O 2157/91

14) Wirksamkeit der Abtretung einer ärztlichen Honorarforderung an eine Verrechnungsstelle
Gericht: BGH
Datum: 10.07.1991
Aktenzeichen: VIII ZR 296/90

15) Geheimnisschutz für die Tätigkeit eines bei einer psychologischen Beratungsstelle angestellten Berufspsychologen auch gegenüber seinem Arbeitgeber
Gericht: BAG
Datum: 13.01.1987
Aktenzeichen: 1 AZR 267/85

16) Zur Verpflichtung und Befugnis des Kassen- und Vertragsarztes, der KÄV zum Zwecke der Qualitätsprüfung Röntgenaufnahmen mit den dazugehörenden Befunden vorzulegen
Gericht: BSG
Datum: 19.11.1985
Aktenzeichen: 6 RKa 14/83

17) Umfang des Zeugnisverweigerungsrechts des Arztes und seiner Berufsgehilfen
Gericht: BGH
Datum: 20.02.1985
Aktenzeichen: 2 StR 561/84

18) Zeugnisverweigerungsrecht des Verwaltungsdirektors eines Krankenhauses
Gericht: OLG Oldenburg
Datum: 10.06.1982
Aktenzeichen: 2 Ws 204/82

19) Umfang der ärztlichen Schweigepflicht
Gericht: OVG Lüneburg
Datum: 29.07.1975
Aktenzeichen: II OVG A 78/73

20) Beschlagnahme einer Karteikarte; Grundrecht auf Achtung des privaten Bereichs
Gericht: BVerfG
Datum: 08.03.1972
Aktenzeichen: 2 BvR 28/71

21) Schweigepflicht ärztlicher Gehilfen
Gericht: LG Köln

Datum: 02.04.1959
Aktenzeichen: 34 Qs 76/59

7. Auftragsdatenverarbeitung und Forschung

Die Frage, wie personenbezogene Daten für Forschungszwecke aus datenschutzrechtlicher Sicht genutzt werden dürfen, beantworten insbesondere die Forschungsregelungen in den jeweils geltenden Datenschutzgesetzen[19], z. B. für private Stellen §40 in Verbindung mit §29 Abs. 6 S.1 Ziff. 4 BDSG. Die unterschiedlichen landesrechtlichen Regelungen beinhalten weitestgehend identische Anforderungen[19]:

- Forschungsdaten unterliegen einer absoluten Zweckbindung, d. h. dürfen für keinen anderen Zweck genutzt werden (§40 Abs. 1 BDSG).
- Die Daten sind zum frühestmöglichen Termin zu anonymisieren bzw. pseudonymisieren.
- Referenzlisten sind separat zu führen (§40 Abs. 2 BDSG).
- Eine personenbezogene Veröffentlichung kommt nur bei Einwilligung oder Ereignissen der Zeitgeschichte in Betracht (§40 Abs. 3 BDSG).
- Forschungsprojekte können auf Basis einer Verhältnismäßigkeitsprüfung auch personenbezogen durchgeführt werden (§28 Abs. 3 Nr. 4, Abs. 6 Nr. 4 BDSG); in diesem Fall sehen Landesregelungen teilweise Melde- und Genehmigungspflichten vor.

Natürlich gelten auch die nicht-forschungsspezifischen datenschutzrechtlichen Regelungen wie etwa die Pflicht zur Datenvermeidung/Datensparsamkeit oder zur Auftragsdatenverarbeitung bzw. die Einschränkungen zu Übermittlungen von Daten ins Ausland[19].

7.1 Anonymisierung/Pseudonymisierung

In der Forschung werden häufig pseudonymisierte Datensätze verwendet, seltener anonymisierte Datensätze. Für die Beantwortung der Frage, ob Daten als pseudonymisiert oder anonymisiert anzusehen sind, ist nach Meinung der Aufsichtsbehörden „immer das gesamte (potenzielle) (Zusatz-) Wissen der verantwortlichen Stelle relevant“[19]: „jedes potenzielle Zusatzwissen ist relevant, auch wenn dieses nur auf unzulässige Weise erlangt werden kann und nur bei (grundsätzlich erreichbaren) dritten Stellen vorhanden ist“.
Entsprechend den Begriffsbestimmungen in §3 BDSG ist

- (6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
- (6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

[19] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2012) Aktuelle Herausforderungen des Datenschutzes im Bereich der medizinischen Forschung. [Online, zitiert am 2014-10-03]; Verfügbar unter https://www.datenschutzzentrum.de/vortraege/20120328-weichert-medizinische-forschung.html

Sowohl das Anonymisieren wie auch das Pseudonymisieren stellen somit eine Verarbeitung personenbezogener Daten im Sinne von §3 Abs. 4 BDSG dar. Entsprechend §4 Abs. 1 ist somit eine Anonymisierung oder Pseudonymisierung nur zulässig, wenn Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Erlaubnistatbestände des BDSG sowie der jeweiligen Landesgesetze bzgl. Verarbeitung und Nutzung von personenbezogenen Daten zu Forschungszwecken können eine entsprechende Rechtsgrundlage zur Pseudonymisierung bzw. Anonymisierung darstellen.

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt weist auf seiner Webseite darauf hin, dass auf der nationalen Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2014 in Hamburg beschlossen wurde, medizinischen Forschungseinrichtungen und -verbünden die neuen generischen Datenschutzkonzepte der TMF als Basis für die konkrete Ausgestaltung von Datenschutzkonzepten zu empfehlen[20]. Dieser Beschluss ist jedoch auf den Webseiten der Datenschutzaufsichtsbehörden, auf denen die Entschließungen der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder dargestellt werden, wie beispielsweise dem BfDI (http://www.bfdi.bund.de/DE/Entschliessungen/DSBundLaender/DSBundLaender_node.html) oder beim Landesbeauftragten für den Datenschutz Rheinland-Pfalz (https://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb), nicht zu finden.

7.2 Rechtsgutachten der TMF

Das vom TMF (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.) beauftragte Rechtsgutachten zur Sekundärnutzung medizinischer Behandlungsdaten kommt zu dem Schluss, dass „eine effektive Pseudonymisierung innerhalb der Behandlungseinrichtung den Personenbezug der an den Auftragnehmer übertragenen pseudonymen Daten“ unter der Voraussetzung, dass die Zuordnung des Pseudonyms zur Person des Patienten nicht an einen Auftragnehmer weitergegeben, sondern geheim gehalten wird, ausschließt[21]. Aus Sicht der Autoren des Rechtsgutachtens führt dies dazu, dass „weder eine Übertragung personenbezogener Daten an den Auftragnehmer i. S. d. Datenschutzrechts stattfindet, welche als Datenübermittlung oder Auftragsdatenverarbeitung zu qualifizieren und zu rechtfertigen wäre, noch ein Offenbaren von Patientengeheimnissen nach §203 StGB“ erfolgt[21]. Aus diesem Gedankengang schließen die Autoren der Studie, dass damit keine gesetzliche Grundlage und auch keine Einwilligung oder Schweigepflichtentbindung des Patienten für diesen Vorgang erforderlich ist.

Die Autoren des Rechtsgutachtens erkennen aber auch, dass Risiken für eine Re-Identifikation bestehen bleiben, sodass eine Re-Identifikation nicht ausgeschlossen werden kann. Die Autoren empfehlen, diese Risiken durch Maßnahmen zu minimieren, die sich zumindest an den Vorschriften über die Auftragsdatenverarbeitung orientieren, ohne diese jedoch zwingend in jedem einzelnen Punkt, insbesondere im Hinblick auf die besonderen Restriktionen der Landeskrankenhausgesetze, vollständig erfüllen zu müssen.

[20] Landesbeauftragter für den Datenschutz Sachsen-Anhalt (2014) Leitfaden zum Datenschutz in medizinischen Forschungsprojekten. [Online, zitiert am 2014-10-03]; Verfügbar unter http://www.datenschutz.sachsen-anhalt.de/service/sonstige-infos/leitfaden-zum-datenschutz-in-medizinischen-forschungsprojekten/

[21] TMF (2014) Sekundärnutzung medizinischer Behandlungsdaten. Publikation in Vorbereitung

7.3 Forschung und Auftragsdatenverarbeitung

Sowohl für personenbezogene wie auch für pseudonymisierte Daten gelten die datenschutzrechtlichen Regelungen. D. h. der Herr der Daten muss prüfen, inwieweit bei einer Weitergabe dieser Daten eine Funktionsübertragung oder eine Auftragsdatenverarbeitung vorliegt. Bei einer Funktionsübertragung ist die Einwilligung eines jeden Betroffenen eine zwingende Voraussetzung zur Datenweitergabe, bei einer Auftragsdatenverarbeitung ist das Vorliegen eines entsprechenden ADV-Vertrags erforderlich.

8. Vorbedingungen für einen ADV-Auftrag

Generell gilt, dass der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen bzw. personenbeziehbaren Daten sorgfältig auszuwählen ist. Diese Anforderung ergibt sich, unabhängig davon, dass sie so auch im Gesetz (§11 Abs. 2 BDSG) steht, schon allein aus der Tatsache, dass es sich bei Gesundheitsdaten um die „besondere Art“ personenbezogener Daten handelt, für die ein entsprechend hoher Schutzbedarf gilt.

Eine Auswahl kann nur als „sorgfältig“ getroffen angesehen werden, wenn die Auswahl mit dem Zweck der Auswahl eines Dienstleisters mit einem angemessenen Datenschutzniveau auszuwählen, geschah[22]. Das Kriterium „der einzige Anbieter“ ist also nicht hinreichend, damit ein ADV-Vertrag abgeschlossen werden darf.

Allerdings ist die Auswahl des Dienstleisters für die Wartung von Systemen der Medizintechnik oder von Systemen der Informationstechnologie in der Regel eingeschränkt. D. h. es steht ausschließlich der Hersteller des jeweiligen Systems für die Wartung zur Verfügung, da kein anderer die für eine Wartung notwendigen Kenntnisse des Systems besitzt. Ist daher eine Nutzung des Systems ohne Wartung nicht möglich bzw. muss eine Nutzung des Systems ohne Wartung als potentiell patientengefährdend eingestuft werden, kann daraus folgen, dass das System gegen das System eines anderen Herstellers gewechselt werden muss, wenn die Voraussetzung zum Abschluss eines Wartungsvertrages beim derzeitigen Hersteller nicht gegeben ist.

In einigen Gesetzen werden Anforderungen gestellt, an deren Erfüllung die Vergabe eines Auftrags an eine Stelle außerhalb der Einrichtung verknüpft ist. D. h., die Verarbeitung von Patientendaten im Auftrag ist nur zulässig, wenn:

a) sonst Störungen im Betriebsablauf nicht vermieden werden können,
b) Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können,
c) die für den Auftraggeber zuständige Aufsichtsbehörde vor Auftragsvergabe um Erlaubnis gebeten wurde oder
d) die für den Auftraggeber zuständige Aufsichtsbehörde vor Auftragsvergabe informiert wurde.

Hier eine Auflistung, in welchem Bundesland welche Anforderungen gelten:

[22] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 55, 56 zu §11

	Baden-Württemberg (§48 LKHG)	Bayern (Art. 27 Absatz 4 BayKHG)	Berlin (§24 Abs. 7 LKG)	Brandenburg (§11 BbgDSG)	Bremen (§10 BremKHDSG)	Hamburg (§9 HmbKHG)	Hessen (§4 HDSG i.V.m. §11 HKHG)	Mecklenburg-Vorpommern (§39 LKHG M-V)
Vermeidung Störungen Betriebsablauf	-	-	-	-	-	-	-	X
Kostengünstigere Abwicklung DV	-	-	-	-	-	-	-	X
Vorab Genehmigung Behörde	-	-	-	-	-	-	-	-
Vorab Information Aufsichtsbehörde	X[1)]	-	X[2)]	-	-	-	-	X
Schweigepflicht entspr. §203 StGB	X	-	-	X	-	-	X	-

1) Gilt für Rechenzentren
2) Gilt für alle Krankenhäuser Berlins, jedoch gelten für andere Gesundheitseinrichtungen die Vorgaben des Landesdatenschutzgesetzes nur für öffentliche Auftraggeber

	Niedersachsen	Nordrhein-Westfalen (GDSG NW)	Rheinland-Pfalz (§36 Abs. 9 LKG)	Saarland (§13 Abs. 7 LKG)	Sachsen (§33 Abs. 10 SächsKHG)	Sachsen-Anhalt (§8 DSG-LSA)	Schleswig-Holstein (§17 LDSG)	Thüringen (§27b ThürKHG)
Vermeidung Störungen Betriebsablauf	-	X	-	X	-	-	-	X
Kostengünstigere Abwicklung DV	-	X	-	X	-	-	-	X
Vorab Genehmigung Behörde	-	-	X	-	X	-	-	-
Vorab Information Aufsichtsbehörde	(X)	-	-	-	-	-	-	X
Schweigepflicht entspr. §203 StGB	-	X	X	-	X	-	-	X

Hinweis für Stellen, die dem Sozialgeheimnis unterliegen:

Bzgl. der Informationspflicht der Aufsichtsbehörde ist anzumerken, dass entsprechend §80 Abs. 3 SGB X der Auftraggeber vor der Erteilung einer Verarbeitung von *Sozialdaten im Auftrag* dies schriftlich der für ihn zuständigen Aufsichtsbehörde anzuzeigen hat. Entsprechend §80 Abs. 5 die „*Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht öffentliche Stellen ist nur zulässig, wenn*

1) *beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder*
2) *die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nichtöffentliche Auftragnehmer weitergibt, verbleiben.“*

Somit sind – abgesehen von der Forderung bzgl. einer Genehmigung durch die für den Auftraggeber zuständige Aufsichtsbehörde sowie der Gewährleistung der aus §203 StGB resultierenden Schweigeverpflichtung – alle landesrechtlichen Anforderungen auch zu erfüllen, wenn Sozialdaten verarbeitet werden. Ein Auftraggeber muss diese Anforderungen des SGB X nur dann nicht beachten, wenn mit absoluter Sicherheit ausgeschlossen werden kann, dass Sozialdaten verarbeitet werden.

8.1 Literatur

1) Bierekoven C. (2012) Aktuelle Entwicklungen zur Auftragsdatenverarbeitung - Präzisierte Anforderungen der Datenschutzaufsichtsbehörden. ITRB: 280-282
2) Conrad I, Fechtner S. (2013) IT-Outsourcing durch Anwaltskanzleien nach der Inkasso-Entscheidung des EuGH und dem BGH, Urteil vom 7.2.2013. CR: 137-148
3) Dix A, Gardain AM. (2006) Datenexport in Drittstaaten - Neue Wege zur Gewährleistung ausreichender Datenschutzgarantien. DuD: 343-346

4) Eckhardt J. (2013) Auftragsdatenverarbeitung. DuD: 585-591
5) Erd R. (2011) Auftragsdatenverarbeitung in sicheren Drittstaaten - Plädoyer für eine Reform von §3 Abs. 8 Satz 3 BDSG. DuD: 275278
6) Fischer TH, Steidle R. (2009) Brauchen wir neue EG-Standardvertragsklauseln für das „Global Outsourcing“?. CR: 632-637
7) Funke M, Wittmann J. (2013) Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung? Anforderungen an die verantwortliche Stelle. ZD: 221-228
8) Hoeren T. (2010) Das neue BdSg und die Auftragsdatenverarbeitung. DuD: 688-691
9) Legerlotz C. (2012) Datenübermittlung und -verarbeitung im Konzern. ArbRB: 190-193
10) Lensdorf L. (2010) Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern - Besonderheiten der neuen EU-Standardvertragsklauseln. CR: 735-741
11) Moos F. (2010) Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010. CR: 281-286
12) Oetterich D. (2012) Keine Auftragsdatenverarbeitung bei Übernahme der Lohn- und Gehaltsabrechnung durch Steuerberater. DStR: 1771-1772
13) Schmidl M, Kone D. (2010) Standardvertragsklauseln als Basis intra-europäischer Auftragsdatenverarbeitung. DuD: 838-843
14) Scholz M, Lutz H. (2011) Standardvertragsklauseln für Auftragsverarbeiter und §11 BDSG Ein Plädoyer für die Unanwendbarkeit der §§11 Abs. 2, 43 Abs. 1 Nr. 2b) BDSG auf die Auftragsverarbeitung außerhalb des EWR. CR: 424-428
15) Schröder M. (2012) Franchising als Auftragsdatenverarbeitung? Rechtliche Fragen bei der Datenübermittlung in einem Franchisenetzwerk. ZD: 106ff
16) Voigt P. (2012) Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland? ZD: 546ff
17) Wanagas S. (2010) Ein Jahr BDSG-Novelle II – Rückblick unter besonderer Berücksichtigung der Fragen der Auftragsdatenverarbeitung und der Informationspflichten. DStR: 1908-1911
18) Weber M, Voigt P (2011) Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. ZD: 74ff

9. Zusammenfassung der Anforderungen an den ADV-Vertrag

Unter Beachtung von §11 BDSG, §80 SGB X[23], den landesrechtlichen sowie kirchlichen gesetzlichen Regelungen ergeben sich die in den folgenden Abschnitten dargestellten Anforderungen, die im ADV-Vertrag geregelt werden müssen.

9.1 Zu regelnde Vertragsbestandteile

1. Gegenstand und Dauer des Auftrags
2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen
3. Ort der Leistungserbringung

Die Landesgesetze für Krankenhäuser schreiben in der Regel vor, dass die

[23] §80 SGB X gilt nur für in §35 SGB I genannte Personen/Stellen, welche Sozialdaten im Sinne von §67 Abs. 1 SGB X verarbeitet (siehe auch Kapitel 9.2 „Besonderheiten bei der Verarbeitung von Sozialdaten im Auftrag“)

Leistungserbringung durch den Auftragnehmer in der Regel beim Auftraggeber zu erfolgen hat, bzw. in einem anderen Krankenhaus erfolgen muss. Im Einzelnen gilt:

a. Baden-Württemberg
   Entsprechend §48 Abs. 1 LKHG Baden-Württemberg sind Patientendaten im Krankenhaus oder im Auftrag des Krankenhauses durch ein anderes Krankenhaus zu verarbeiten. Außerhalb eines Krankenhauses dürfen Patientendaten nur verarbeitet werden, wenn die Anforderungen aus §48 Abs. 1 LKHG Baden-Württemberg erfüllt sind. Hierzu gehört u. a., dass der Auftragnehmer seinen Mitarbeitern eine §203 StGB entsprechende Schweigepflicht auferlegt. Weiterhin müssen sich die Patientendaten zu jedem Zeitpunkt im ausschließlichen Gewahrsam des Krankenhauses, in dessen Auftrag sie verarbeitet werden, befinden.

b. Bayern
   Gemäß Art. 27 Abs. 4 S. 6 BayKrG darf sich ein Krankenhaus zur *„Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind“* nur anderer Krankenhäuser bedienen.

c. Berlin
   Entsprechend §24 Abs. 7 LKG Berlin gilt, dass Patientendaten *„grundsätzlich im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus zu verarbeiten“* sind. Andere Stellen, d. h. Stellen, die selbst kein Krankenhaus sind, dürfen Patientendaten im Auftrag eines Krankenhauses nur verarbeiten, wenn durch technische Schutzmaßnahmen gewährleistet ist, dass der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen.

d. Brandenburg
   In Brandenburg gibt es keine datenschutzrechtliche Spezialgesetzgebung bzgl. Datenverarbeitung im Auftrag für Krankenhäuser.

e. Bremen
   Laut §10 Abs. 1 BremKHDSG sind Patientendaten grundsätzlich im Krankenhaus zu verarbeiten. Jedoch ist eine Verarbeitung im Auftrag zulässig, *„wenn die Wahrung der Datenschutzbestimmungen dieses Gesetzes bei der verarbeitenden Stelle sichergestellt ist und diese sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft“*.

f. Hamburg
   Gemäß §9 Abs. 1 HmbKHG darf ein Krankenhaus eine Stelle außerhalb des Krankenhauses mit der Speicherung und der weiteren Verarbeitung von Patientendaten beauftragen.

g. Hessen
   Das Hessische Krankenhausgesetz hat keine spezialgesetzliche Regelung bzgl. Datenverarbeitung im Auftrag, verweist in §12 Abs. 1 HKHG aber auf die Bestimmungen des Hessischen Datenschutzgesetzes. §4 HDSG regelt die Verarbeitung personenbezogener Daten im Auftrag und gemäß §4 Abs. 2 S. 5 HDSG darf an nicht-öffentliche Stellen ein Auftrag nur vergeben werden, wenn

„weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen“.

h. Mecklenburg-Vorpommern
Laut §39 LKHG M-V darf ein Krankenhaus eine Verarbeitung von Patientendaten einem Auftragnehmer nur dann übertragen, wenn
- Störungen im Betriebsablauf sonst nicht vermieden werden können,
- die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
- das Krankenhaus seinen Betrieb einstellt.

Ist eine Verarbeitung unter diesen Bedingungen jedoch erlaubt, existieren keine Bestimmungen bzgl. des Ortes der Datenverarbeitung, jedoch eine zeitliche. Es gilt die Bestimmung, dass eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses nur zulässig ist, „wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt“.

i. Niedersachsen
In Niedersachsen gibt es keine datenschutzrechtliche Spezialgesetzgebung bzgl. Datenverarbeitung im Auftrag für Krankenhäuser.

j. Nordrhein-Westfalen
Gemäß §7 Abs. 1 Gesundheitsdatenschutzgesetz NRW sind Patientendaten *„grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten“*. Entsprechend §7 Abs. 2 GDSG NW ist eine *„Verarbeitung von Patientendaten im Auftrag ist nur zulässig, wenn sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können“*, jedoch muss sich der Auftraggeber vor Auftragsvergabe beim Auftragnehmer vergewissern, dass *„die Wahrung der Datenschutzbestimmungen dieses Gesetzes und der ärztlichen Schweigepflicht sichergestellt ist“*.

k. Rheinland-Pfalz
Laut §36 Abs. 9 LKG Rheinland-Pfalz darf sich ein Krankenhaus *„zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn die Einhaltung der Datenschutzbestimmungen dieses Gesetzes sowie eine §203 StGB entsprechende Schweigepflicht bei der Auftragnehmerin oder beim Auftragnehmer sichergestellt ist“* und die zuständige Behörde der Auftragserteilung zustimmte. Bzgl. der örtlichen Verarbeitung gibt es keine weitergehenden Vorgaben.

l. Saarland
Entsprechend §13 Abs. 7 Saarländisches Krankenhausgesetz darf ein Krankenhaus Patientendaten von Personen und Stellen außerhalb des Krankenhauses im Auftrag nur verarbeiten lassen, *„wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der Datenverarbeitung hierdurch kostengünstiger besorgt werden können“*. Bzgl. des Ortes der Leistungserbringung finden sich im Saarländischen Krankenhausgesetz keine weiteren Vorgaben.

m. Sachsen

§33 Abs. 10 SächsKHG fordert, dass sich ein Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen nur bedienen darf, *„wenn sichergestellt ist, dass diese die Datenschutzbestimmungen dieses Gesetzes und die §203 Strafgesetzbuch entsprechende Schweigepflicht einhalten“* und die zuständige Behörde der Auftragserteilung zustimmte. Weitergehende Bestimmungen bzgl. des Ortes der Leistungserbring finden sich im SächsKHG nicht.

n. Sachsen-Anhalt
In Sachsen-Anhalt gibt es keine datenschutzrechtliche Spezialgesetzgebung bzgl. Datenverarbeitung im Auftrag für Krankenhäuser.

o. Schleswig-Holstein
In Schleswig-Holstein gibt es keine datenschutzrechtliche Spezialgesetzgebung bzgl. Datenverarbeitung im Auftrag für Krankenhäuser.

p. Thüringen
§27b des Thüringer Krankenhausgesetz (ThürKHG) enthält die Vorschriften für eine Datenverarbeitung im Auftrag. Demgemäß (§27b Abs.1 ThürKHG) sind Patientendaten grundsätzlich im Krankenhaus zu verarbeiten. Eine Auftragsdatenverarbeitung ist nur zulässig, wenn:
  - *„sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können,*
  - *die Einhaltung der Datenschutzbestimmungen dieses Gesetzes sowie eine den Voraussetzungen des §203 des Strafgesetzbuchs entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist und*
  - *der Auftraggeber der Aufsichtsbehörde nach §32 Abs. 2 rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich angezeigt hat“*.

Weitergehende Anforderungen bzgl. des Ortes der Leistungserbringung finden sich im Gesetz nicht.

4. Die zu treffenden technischen und organisatorischen Maßnahmen
   a. Anlage zu §9 BDSG bzw. §78 SGB X: Maßnahmen um

      - Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
      - zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
      - zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
      - zu gewährleisten, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung

von Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- zu gewährleisten, dass Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),
- zu gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

b. Berlin
   - Protokollierungspflicht

5. Die Berichtigung, Löschung und Sperrung von Daten

6. Die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen

   a. Berlin
      - Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,
      - Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,
      - Daten dürfen ausschließlich für den Zweck der Wartung verwendet werden,
      - sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt,
      - sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgen kann,
      - zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden,
      - die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
      - Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik und
      - sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,
      - zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,
      - zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können

   b. Baden-Württemberg
      - der Auftragnehmer erlegt seinen Mitarbeitern, soweit ihnen aus zwingenden Gründen eine Zugriffsberechtigung auf Patientendaten eingeräumt wird, eine §203 StGB entsprechende Schweigepflicht auf

   c. Nordrhein-Westfalen

- Patientendaten aus dem ärztlichen Bereich sind vom Auftragnehmer auf physisch getrennten Dateien zu verarbeiten

d. Rheinland-Pfalz
   - die Einhaltung einer §203 StGB entsprechenden Schweigepflicht beim Auftragnehmer muss sichergestellt sein.

e. Sachsen
   - Beim Auftragnehmer muss eine §203 Strafgesetzbuch entsprechende Schweigepflicht gewährleistet sein

f. Thüringen
   - Eine §203 des Strafgesetzbuchs entsprechende Schweigepflicht muss beim Auftragnehmer sichergestellt sein.

g. Evangelische Kirche
   - Beim Auftragnehmer die auch §203 StGB resultierenden Geheimhaltungspflichten gewährleistet sind.

h. Katholische Kirche
   - Beim Auftragnehmer die auch §203 StGB resultierenden Geheimhaltungspflichten gewährleistet sind.

7. Pflichten des Auftraggebers

a. Berlin
   - sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können,
   - die technische Verbindung muss vom Auftraggeber hergestellt werden; sofern dies nicht möglich ist, ist ein Rückrufverfahren verbindlich festzulegen,
   - Anwesenheit des Systemverwalters ist möglichst sicherzustellen,

b. Baden-Württemberg
   - Die Wartung muss immer vom Auftraggeber beauftragt werden, der Auftragnehmer darf nur auf ausdrückliche Weisung des Auftragnehmers handeln.

c. Bremen
   - Die Wartung muss immer vom Auftraggeber beauftragt werden, der Auftragnehmer darf nur auf ausdrückliche Weisung des Auftragnehmers handeln.

d. Mecklenburg-Vorpommern
   - Eine Abschrift des ADV-Vertrages hat der Krankenhausträger dem Landesbeauftragten für den Datenschutz unverzüglich zu übersenden

e. Nordrhein-Westfalen
   - Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs des GDSG NW ist die zuständige Datenschutzkontrollbehörde zu unterrichten

f. Sachsen
   - Die Auftragserteilung bedarf der vorherigen Zustimmung durch die zuständige Behörde.

g. Thüringen
   - Der Auftraggeber muss der Aufsichtsbehörde rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich anzeigen.

8. Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen

a. Berlin
   - für den Fall, dass ein Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union tätig wird, sind stets die jeweiligen Regelungen des §14 BlnDSG über die Übermittlung personenbezogener Daten an ausländische und internationale Stellen anzuwenden.

b. Mecklenburg-Vorpommern
   - Eine Übertragung des Auftrags auf Dritte oder die Erteilung von Unteraufträgen ist nur mit Zustimmung des Krankenhausträgers zulässig

9. Die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers

a. Baden-Württemberg
   - Zuständige Aufsichtsbehörde ist Aufsichtsbehörde des Auftraggebers

b. Bremen
   - Zuständige Aufsichtsbehörde ist Aufsichtsbehörde des Auftraggebers

c. Mecklenburg-Vorpommern
   - Zuständige Aufsichtsbehörde ist Aufsichtsbehörde des Auftraggebers

d. Nordrhein-Westfalen
   - Zuständige Aufsichtsbehörde ist Aufsichtsbehörde des Auftraggebers

e. Sachsen-Anhalt
   - Der Auftragnehmer unterwirft sich der Kontrolle durch den Landesbeauftragten für den Datenschutz.

f. Thüringen
   - Im ADV-Vertrag ist sicherzustellen, dass vom Auftraggeber oder von dessen Datenschutzkontrollbehörde veranlasste Kontrollen vom Auftragnehmer jederzeit zu ermöglichen sind.

g. Evangelische Kirche
   - Der Auftragnehmer muss sich der Kontrolle kirchlicher Datenschutzbeauftragter unterwerfen.

10. Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder gegen die im Auftrag getroffenen Festlegungen

11. Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält

12. Die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags

    a. Berlin
        - Löschung der Daten nach Abschluss der Wartungsarbeiten

9.2 Besonderheiten bei der Verarbeitung von Sozialdaten im Auftrag

Die Legaldefinition von „Sozialdaten“ findet sich in §67 Abs. 1 SGB X:

> *„… Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in §35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden …“*

D. h. Sozialdaten sind Daten, die von in den §§18 - 29 SGB I genannten Stellen, dies sind

- öffentlichen Vereinigungen,
- Integrationsfachdienste,
- die Künstlersozialkasse,
- die Deutsche Post AG,
- Behörden der Zollverwaltung,
- Versicherungsämter,
- Gemeindebehörden,
- anerkannte Adoptionsvermittlungsstellen nach §2 Abs. 2 des Adoptionsvermittlungsgesetzes sowie
- die Stellen, welche Aufgaben nach §67c Abs. 3 SGB X wahrnehmen,

erhoben, verarbeitet oder genutzt werden. Für diese Daten gilt der Sozialdatenschutz; entsprechend ist eine Verarbeitung von Sozialdaten insbesondere nur nach den Maßgaben von §80 SGB X zulässig. Damit unterliegen Daten der Leistungserbringer wie beispielsweise Krankenhäuser oder Arztpraxen grundsätzlich nicht dem Sozialdatenschutz.

Entsprechend §67a Abs. 2 können Sozialdaten direkt beim Leistungserbringer erhoben werden. Damit können Krankenhäuser/Arztpraxen Sozialdaten z. B. für eine Krankenkasse erheben und die Daten an diese entsprechend den gesetzlichen Grundlagen der Sozialgesetzbücher übermitteln. Für die Übermittlung muss selbstverständlich ein Schutz der Daten gewählt werden, der den Anforderungen zum Schutz von Sozialdaten entspricht. Jedoch werden die Daten beim Leistungserbringer, die ursprünglich zu Zwecken der Patientenversorgung erhoben wurden, nicht zu Sozialdaten. Die empfangende Stelle, d. h. eine Stelle entsprechend §§18 - 29 SGB I, hingegen unterliegt dem Sozialdatenschutz.

Will eine Stelle nach §§18 - 29 SGB I eine Auftragsdatenverarbeitung durchführen, so muss Sie beachten, dass die Anforderungen von §80 Abs. 3, 4 und 5 SGB X sich von den Anforderungen des BDSG unterscheiden.

9.2.1 §80 Abs. 3 SGB X

Gemäß §80 Abs. 3 SGB X muss der Auftraggeber vor Auftragsvergabe seine Aufsichtsbehörde schriftlich informieren über

- den Auftragnehmer, die bei diesem vorhandenen technischen und organisatorischen Maßnahmen und ergänzenden Weisungen nach §80 Abs. 2 Satz 2 und 3 SGB X,
- die Art der Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden sollen, und den Kreis der Betroffenen,
- die Aufgabe, zu deren Erfüllung die Erhebung, Verarbeitung oder Nutzung der Daten im Auftrag erfolgen soll, sowie
- den Abschluss von etwaigen Unterauftragsverhältnissen.

9.2.2 §80 Abs. 4 SGB X

Laut §80 Abs. 4 SGB X ist es dem Auftragnehmer verboten, die zur Datenverarbeitung überlassenen Sozialdaten für andere Zwecke zu verarbeiten oder zu nutzen oder länger zu speichern, als der Auftraggeber schriftlich bestimmte.

9.2.3 §80 Abs. 5 SGB X

Entsprechend §80 Abs. 5 SGB X ist eine Verarbeitung von Sozialdaten im Auftrag durch nicht öffentliche Stellen nur zulässig, wenn

- *„beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder*
- *die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben“.*

9.2.4 Zu treffende vertragliche Regelungen gemäß §80 Abs. 2 SGB X

Die geforderten vertraglichen Regelungen von §80 SGB X und §11 BDSG entsprechen sich wiederum:

Zu regelnder Vertragsbestandteil	BDSG	SGB X
Der Gegenstand und die Dauer des Auftrags	§11 Abs. 2 Ziff. 1 BDSG	§80 Abs. 2 Ziff. 1 SGB X
Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen	§11 Abs. 2 Ziff. 2 BDSG	§80 Abs. 2 Ziff. 2 SGB X
Die nach §9 BDSG zu treffenden technischen und organisatorischen Maßnahmen	§11 Abs. 2 Ziff. 3 BDSG	
Die nach §78a SGB X zu treffenden technischen und organisatorischen Maßnahmen		§80 Abs. 2 Ziff. 3 SGB X
Die Berichtigung, Löschung und Sperrung von Daten	§11 Abs. 2 Ziff. 4 BDSG	§80 Abs. 2 Ziff. 4 SGB X
Die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen	§11 Abs. 2 Ziff. 5 BDSG	§80 Abs. 2 Ziff. 5 SGB X
Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen	§11 Abs. 2 Ziff. 6 BDSG	§80 Abs. 2 Ziff. 6 SGB X
Die Kontrollrechte des Auftraggebers und die	§11 Abs. 2 Ziff.	§8 0 Abs. 2

entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers	7 BDSG	Ziff. 7 SGB X
Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen	§11 Abs. 2 Ziff. 8 BDSG	
Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz von Sozialdaten oder gegen die im Auftrag getroffenen Festlegungen		§80 Abs. 2 Ziff. 8 SGB X
Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält	§11 Abs. 2 Ziff. 9 BDSG	§80 Abs. 2 Ziff. 9 SGB X
Die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags	§11 Abs. 2 Ziff. 10 BDSG	§80 Abs. 2 Ziff. 10 SGB X

D. h. die im vorliegenden Muster-ADV-Vertrag vorgeschlagenen Formulierungen können sowohl zur Ausgestaltung eines ADV-Vertrages auf Basis des §80 SGB X wie des §11 BDSG als Basis dienen.

§80 Abs. 2 SGB X kennt nach Ziffer 10 jedoch noch ergänzende Anforderungen, die sich so nicht in §11 BDSG finden lassen. §80 Abs. 2 Satz 3-6 SGB X fordert:

- Der **Auftraggeber** ist **verpflichtet**, erforderlichenfalls **Weisungen** zur Ergänzung **der beim Auftragnehmer vorhandenen technischen** und **organisatorischen Maßnahmen** zu **erteilen**.
- Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
- Das Ergebnis ist zu dokumentieren.
- Die **Auftragserteilung** an **eine nicht-öffentliche Stelle** setzt außerdem voraus, dass der **Auftragnehmer** dem Auftraggeber **schriftlich das Recht eingeräumt** hat,
    - Auskünfte bei ihm einzuholen,
    - während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen und
    - geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen.

Daher muss der Auftraggeber die technischen und organisatorischen Maßnahmen des Auftragnehmers bzgl. der Einhaltung der sozialdatenschutzrechtlichen Anforderungen prüfen und ggfs. Ergänzungen fordern, dementsprechend ist dem Anhang 2 des Muster-ADV-Vertrages besondere Sorgfalt zu erweisen. Weiterhin sind einige im Muster-ADV-Vertrag als „optional“ gekennzeichnete Stellen bei der Sozialdatenverarbeitung im Auftrag nicht optional, entsprechend muss dies bei der Vertragsgestaltung beachtet werden.

Kommentierter Muster-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

……

(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.

Kommentierung Präambel

Wichtig ist die Unterscheidung zwischen der ärztlichen Schweigepflicht entsprechend §203 StGB und dem Schutz personenbezogener Daten resultierend aus den jeweils gültigen Datenschutzgesetzen.

Das Grundrecht auf informationelle Selbstbestimmung wie auch die übrigen Ausprägungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 des Grundgesetzes enden mit dem Tod eines Menschen. Die auf diesem Grundrecht beruhenden datenschutzrechtlichen Bestimmungen gelten daher nicht mehr nach dem Tod des Menschen.

Aus §203 Abs. 3 StGB hingegen ergibt sich, dass ein Arzt, Zahnarzt oder Rechtsanwalt auch noch nach dem Tod seines Patienten oder Klienten zur Verschwiegenheit verpflichtet ist. D. h. bei verstorbenen Patienten gelten zwar die datenschutzrechtlichen Bestimmungen nicht länger, aber die ärztliche Schweigepflicht dauert weiter an.

Weiterhin ist zu beachten, dass §203 StGB die unbefugte Offenbarung von Patientengeheimnissen unter Strafe stellt, auch wenn die Tat nur auf Antrag des Betroffenen verfolgt wird. Viele auf Strafrecht spezialisierte Juristen sehen im Datenschutzrecht keine Befugnis zur Offenbarung von Patientengeheimnissen. In der Tat steht z. B. in §1 Abs. 3 S. 2 BDSG: *„Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt“*.

Damit existiert in Deutschland das Paradoxon, dass eine Arztpraxis oder ein Krankenhaus eine datenschutzrechtlich einwandfrei geregelte Form der externen Erbringung von Leistungen („Outsourcing“) betreiben kann, jedoch eventuell gegen geltendes Strafrecht verstößt.

Diesen Widerspruch kann auch ein ADV-Vertrag nicht auflösen. Dies kann nur durch eine entsprechende gesetzliche Regelung seitens des Gesetzgebers geklärt werden oder die unterschiedlich beurteilte Frage, ob eine datenschutzrechtlich erlaubte Auftragsverarbeitung einen Befugnistatbestand darstellt, wird höchstrichterlich geklärt.

In diesem Muster-ADV-Vertrag werden daher nur die reinen datenschutzrechtlichen Bestandteile besprochen. Festzuhalten ist allerdings, dass für die Einhaltung der strafrechtlichen Bestimmungen der Auftraggeber, also die Einrichtung der Gesundheitsversorgung, verantwortlich ist und diese Verantwortung auch nicht an den Auftragnehmer delegieren kann.

Delegiert werden kann hingegen, dass der Auftragnehmer das bei ihm beschäftigte Personal auf die besondere Sensibilität der Daten hinweist und auf den besonderen Schutz, denen diese Daten unterliegen. Ggfs. können auch haftungsrechtliche Strafen vereinbart werden, wenn es zu einer rechtlich nicht zu rechtfertigenden Offenbarung der Patientendaten seitens des Auftragnehmers kommt.

Formelle Verpflichtung der Auftragsdatenverarbeitenden

In der Regel wird der Auftragnehmer dem von ihm eingesetzten Personal keine §203 StGB entsprechende Schweigepflicht auferlegen können, da der Auftragnehmer in seiner datenschutzrechtlichen Verpflichtung keine strafrechtliche Komponente integrieren kann.

Das „Gesetz über die förmliche Verpflichtung nichtbeamteter Personen“ (Verpflichtungsgesetz) sieht jedoch genau diese strafrechtliche Komponente vor. Die jeweiligen Bundesländer haben in ihren jeweiligen Verordnungen beschrieben, wer eine entsprechende Verpflichtung vollziehen kann. Die Mehrzahl der Auftragnehmer wird

vermutlich keine Verpflichtung nach dem Verpflichtungsgesetz durchführen dürfen, jedoch wird diese Möglichkeit für einige (öffentliche) Auftraggeber gegeben sein.
Wenn möglich sollte eine entsprechende Verpflichtung des vom Auftragnehmer eingesetzten Personals entsprechend dem Verpflichtungsgesetz durchgeführt werden, sei es vom Auftraggeber oder vom Auftragnehmer.

Verpflichtung nach §17 UWG

Der Auftragnehmer kann allerdings das von ihm eingesetzte Personal entsprechend §17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) darauf hinweisen, dass schon der Versuch der Weitergabe von Geschäfts- oder Betriebsgeheimnis eine strafbare Handlung darstellt, die mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet werden kann. Da dieses Delikt nur auf Antrag verfolgt wird, sollte der Auftragnehmer das von ihm eingesetzte Personal darauf hinweisen, dass jegliche unbefugte Weitergabe von Patientendaten zu einem Antrag bei der Strafverfolgungsbehörde führen kann.

Literatur

1) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
2) Siebenhüner R. (2013) Wartung technischer Systeme im Krankenhaus durch externe Dienstleister - Datenschutzrechtliche Aspekte. 1. Auflage. Deutsche Krankenhaus Verlagsgesellschaft mbH
3) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand
4) Vander S. (2013) Möglichkeiten und Grenzen weisungsgebundener Datenweitergabe - Beauftragung von IT-Leistungen in geheimnisschutzrelevanten Geschäftsfeldern nach der EuGH-Rechtsprechung. ZD: 492-497

§1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend §2 und §3 BDSG, §2 UWG und §2 TMG sowie Landesdatenschutzgesetz/Landeskrankenhausgesetz [hier bitte das für das jeweils geltende Rechtswerk benennen]. 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).

Kommentierung §1

Generell sollte auf Rechtsnormen verwiesen werden, wenn dort die benötigten Definitionen zu finden sind. Ergänzend werden in diesem Abschnitt die Begrifflichkeiten definiert, welche einerseits für den Vertrag relevant sind, andererseits an anderer Stelle nicht definiert wurden.

In §1 des Muster-ADV-Vertrages wird in den Zeilen 2 - 4 daher auf die im BDSG und TMG enthaltenen Definitionen verwiesen, in den Zeilen 8 - 17 die dort nicht enthaltenen Begriffe „Datenverarbeitung im Auftrag“ sowie „Weisung“ definiert.

Entsprechend dem Verständnis der Artikel 29 Gruppe ist „Anonymisierung als ein auf personenbezogene Daten angewandtes technisches Verfahren nach dem aktuellen Stand der Technik“ anzusehen, d. h. das Ergebnis einer Anonymisierung muss „so dauerhaft sein wie eine Löschung“[24]. Dabei ist ein Anonymisierungsverfahren „als eine Form der Weiterverarbeitung“ personenbezogenen Daten mit dem Ziel ihrer Anonymisierung anzusehen[24]. Daher muss bei einer Anonymisierung „geprüft werden, ob sie das Kriterium der Vereinbarkeit im Sinne der Leitlinien erfüllt, die von der Datenschutzgruppe in ihrer Stellungnahme 03/2013 zur Zweckbindung vorgelegt wurden“[25]. Dementsprechend ist eine Anonymisierung nur erlaubt, wenn mindestens einer der in Artikel 7 der Richtlinie 95/46/EG genannten Gründe zutrifft[24].

Literatur

1) Artikel-29-Datenschutzgruppe. (2007) Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“. [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf
2) Artikel-29-Datenschutzgruppe. (2010) Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf
3) Artikel-29-Datenschutzgruppe. (2011) Stellungnahme 15/2011 zur Definition von Einwilligung. [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

[24] Artikel-29-Datenschutzgruppe (2014) Stellungnahme 5/2014 zu Anonymisierungstechniken. [Online, zitiert am 2014-10-21]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[25] Article 29 Data Protection Working Party. (2013) Opinion 03/2013 on purpose limitation. [Online, zitiert am 2014-10-21]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

§2 Gegenstand, Verantwortlichkeit und Dauer des Auftrags

§2.1 Gegenstand des Auftrags

Alt. 1 zu Abs. 1

(1) Gegenstand der Vereinbarung ist die Erhebung bzw. Verarbeitung oder Nutzung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit … in Ergänzung des … Vertrags der Parteien vom …, (nachstehend „Hauptvertrag“ genannt“). Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt dem Auftragnehmer, folgende personenbezogene Daten zu erheben:

a. Bezeichnung der Daten
   - Personalstammdaten
   - Besondere Datenarten
     - rassische oder
     - ethnische Herkunft,
     - religiöse Überzeugung
     - philosophische Überzeugung
     - politische Überzeugungen / Meinungen
     - Gesundheit
     - Gewerkschaftszugehörigkeit

   Bei den Betroffenen der oben aufgelisteten Daten handelt es sich um:
   - Patienten
   - Kunden
   - Interessenten
   - Abonnenten
   - Beschäftigte
   - Lieferanten
   - Handelsvertreter
   - Ansprechpartner
   - Sonstiges

b. Der Zugriff auf die Daten bzw. die Datenerhebung erfolgt wie folgt:
   - Übermittlung durch den Auftraggeber über: ……
   - Beauftragung durch den Arbeitgeber: ……

   Der Auftragnehmer erbringt für den Auftraggeber folgende Prüf- bzw. Wartungstätigkeiten, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann:
   - Prüfung/Wartung vor Ort: ……
   - Hardware-Diagnose per Fernzugriff für folgende Hardwareprodukt(e): ……
   - Software-Prüfung/Wartung per Fernzugriff für folgend(e) Softwareprodukt(e): ……

Alt. 2 zu Abs. 1

(1) Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

Alt. 3 zu Abs. 1

(1) 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:

Art der Daten	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen

§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

Alt. 1 zu Abs. 1

(1) Die Dauer des Auftrags ist in §… des Hauptvertrags vom … zwischen Auftraggeber und Auftragnehmer geregelt, sofern sich aus den Bestimmungen dieses ADV-Vertrages nicht darüber hinausgehende Verpflichtungen ergeben.

Alt. 2 zu Abs. 1

(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.

Alt. 3 von Abs. 1

(1) 1. Die Laufzeit dieses ADV-Vertrages endet am …, sofern sich aus den Bestimmungen dieses ADV-Vertrages nicht darüber hinausgehende Verpflichtungen ergeben.

Alt. 4 von Abs. 1

(1) Der Vertrag wird mit der Unterzeichnung wirksam und läuft auf unbestimmte Zeit. Jede Partei ist berechtigt, den Vertrag mit einer Frist von … Wochen zum Monatsende/Quartalsende/Jahresende (nicht Zutreffendes streichen) zu kündigen.

(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.

(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.

Opt. (4) Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind

	Nicht Zutreffende bitte ausschließen
Geschäftsführung, Verwaltungsleitung	Nein θ
IT-Leitung	Nein θ
Ärzte	Nein θ
Pflegekräfte, Arzthelferinnen	Nein θ
Weitere vom Auftraggeber mit der Betreuung seiner Daten beauftragte Personen, z.B. regionale Systembetreuer	Nein θ

Opt. §2.5 Leistung durch den Auftragnehmer

Der Auftragnehmer erbringt für den Auftraggeber bezogen auf die in §2 genannten Daten folgende Leistungen:

– …

Opt. 2.6 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland bzw. von den mit dem Auftraggeber in Anhang 1 vereinbarten Leistungsstandorten der Unterauftragnehmer aus 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) Bei einer Leistungserbringung außerhalb Deutschlands (z. B. auch durch (Fernzugriffe aus dem Ausland), sei es aus Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, oder aus anderen Ländern (sog. Drittstaaten), wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern.

(5) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind und über ein dem diesen Vertrag genügendem und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber informiert. Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung über die Verlagerung über schwerwiegende Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(6) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Vertragspartner, der die Verlagerung des Ortes der Leistungserbringung wünscht.

(7) 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.

Kommentierung §2

Gegenstand und Dauer

Meistens wird der genaue Gegenstand des Auftrags in einem Hauptvertrag dargestellt sein, sodass an dieser Stelle auf den entsprechenden Vertrag verwiesen werden kann (§2.1). Gleiches gilt für die Dauer der Beauftragung (§2).

Allerdings muss man hierbei bedenken, dass prüfungsberechtigten Dritten Einblick in datenschutzrechtlich relevante Vereinbarungen zu gewähren ist. Werden ADV- und Hauptvertrag nicht strukturell getrennt, entsteht ggfs. im Fall eines Audits entsprechender Aufwand für das Unkenntlichmachen des Inhalts, welcher der Prüfung des jeweiligen (datenschutzrechtlich) Berechtigten nicht unterliegt.

Der Kreis der Betroffene ist dabei so konkret wie möglich zu erfassen, pauschale Angaben wie „Kundendaten“ verbieten sich[26]. Dabei müssen der Zweck, der betroffene Personenkreis und der beabsichtigte Umgang der Daten einander zuordenbar angegeben werden[22]. D. h. erfolgt der Datenumgang zu unterschiedlichen Zwecken, müssen die Art der Daten und der Kreis der betroffenen Personen jeweils gesondert dem oder den Verwendungszweck(en) zugeordnet werden. Dies kann in einer tabellarischen Aufzählung geschehen, wie in §2.1 dargestellt.

Konkretisierung des Auftrags

Meistens wird im eigentlichen Vertrag nicht auf die datenschutzrechtlichen Aspekte wie beispielsweise der Art der Unterstützung (z. B. Administration der Patientenverwaltung) oder der Nennung der betroffenen Personenpaare (Patienten, Angestellte, Zulieferer usw.) eingegangen, sondern lediglich die technische Funktionalität (beispielsweise durch die Worte „... Gewährleistung der Funktionsfähigkeit der Software XY“) beschrieben. Daher müssen diese Angaben in diesem Abschnitt des ADV-Vertrags (§2.1 und in §2.5) beschrieben werden.

Dauer des Auftrags

Kündigungsbestimmungen sind - abgesehen von den gesetzlichen Anforderungen z. B. in §11 Abs. 2 Ziff. 1 BDSG - in einem ADV-Vertrag eigentlich überflüssig, da sie entweder aufgrund ausdrücklicher Bestimmung im Hauptvertrag oder gemäß §§133 , 157 BGB von einer Beendigung des Hauptvertrags mit erfasst werden.

Gesetzlich vorgeschrieben ist, dass die Dauer und damit auch die Beendigung der ADV-Dienstleistung vertraglich geregelt werden muss. Damit kann die Dauer des Auftrags befristet werden, jedoch kann der Auftrag auch unbefristet erteilt werden. In letzterem Fall muss jedoch die Art und Weise der Beendigung des Vertrages vereinbart werden.

Weisungsbefugnisse des Auftraggebers

Die gesetzlichen Vorschriften schreiben dem Auftraggeber vor, dass in einem ADV-Vertrag der Umgang mit den Daten durch den Auftragnehmer beschrieben werden muss. Insbesondere ist vorgeschrieben, dass der Auftragnehmer nur auf Weisung des Auftraggebers tätig werden darf und dies im Vertrag festgehalten werden muss (§2.4).

Es kann gerade im Gesundheitswesen vorkommen, dass eine schnelle Reaktion des Auftragnehmers erforderlich ist, welche eine vorherige schriftliche Beauftragung nicht ermöglicht, z. B. weil im Nachtdienst keine unterschriftsberechtigte Person eine schriftliche Weisung erteilen kann. Reagiert der Auftragnehmer hier auf eine mündliche Beauftragung seitens des Auftraggebers, um Schaden vom Patienten abzuwenden, so muss der Auftragnehmer unverzüglich eine schriftliche Beauftragung nachreichen. Ohne

[26] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 71 zu §11

entsprechende Weisung ist der Auftragnehmer nicht befugt, Daten in anderer Form zu verarbeiten. Dies muss der Auftragnehmer ggfs. gegenüber der zuständigen Aufsichtsbehörde nachweisen. Daher ist es aus Sicht des Auftragnehmers wichtig, dass jede Weisung schriftlich erfolgt und er so den Nachweis des Tätigwerdens auf Weisung des Auftraggebers gegenüber der Aufsichtsbehörde erbringen kann.

Literatur

1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
2) Eckhardt J. (2013) Auftragsdatenverarbeitung - Gestaltungsmöglichkeiten und Fallstricke. DuD: 585-591
3) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
4) Holländer C. (2014) Auftragsdatenverarbeitung: Aus der Praxis der Aufsichtsbehörden. ITRB: 115-116
5) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
6) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

§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.

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

Opt. (3) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung.

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

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

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

Opt. (11): Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Opt. (12) Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(13) 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.

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

(15) 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.

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

(17) 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.

(18) 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.

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

Opt. (20) Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

Opt. §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 Datenverarbeitungsanlagen werden, 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 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.

Kommentierung §3

§11 BDSG und §80 SGB X[27] schreiben einige Pflichten des Auftraggebers vor, andere ergeben sich aus dem allgemeinen Datenschutzrecht, den landesrechtlichen Bestimmungen wie auch aus dem Haftungsrecht.

Technisch-organisatorische Maßnahmen

Die eigentlichen technisch-organisatorischen Maßnahmen (TOM's), welche der Auftragnehmer zum Schutz der ihm anvertrauten Daten trifft, werden in einem Anhang dargestellt. Hier wird vertraglich festgehalten, dass der Auftragnehmer die Vorschriften des BDSG bzw. des SGB X[27] sowie der entsprechenden landesrechtlichen Vorgaben berücksichtigt und einhält sowie dem Auftraggeber nachweist (§3 Ziff. (2)).

Der Gesetzgeber schreibt vor, dass sich der Auftraggeber vor Auftragsvergabe (und damit insbesondere vor Vertragsabschluss) „überzeugen" muss, nicht jedoch, wie dies genau zu geschehen hat. Im Zweifelsfall muss der Auftraggeber der Aufsichtsbehörde gegenüber den Überzeugungsprozess nachweisen. Daher darf hier keine Beschränkung des Überzeugungsprozesses durch den Auftragnehmer erfolgen, indem beispielsweise eine Überzeugung ausschließlich aufgrund des Nachweises von Zertifikaten erfolgt. (Abgesehen davon hätte speziell diese Regelung den Nachteil, dass der Auftragsdatenverarbeitungsprozess sofort beendet werden müsste, wenn das Zertifikat einmal nicht verlängert würde.)

Verweigert der Auftragnehmer die Umsetzung bzw. Anpassung der aus Sicht des Auftraggebers mindestens zur Gewährleistung des Schutzbedarfs der Patientendaten entsprechenden Maßnahmen, so kann dies die Datenverarbeitung durch den Auftragnehmer rechtswidrig machen. Daher müssen die TOM's entsprechend den sich wandelnden Gegebenheiten angepasst werden können, ohne dass damit der Vertrag als solches geändert werden müsste. Daher wird in §3 Zeilen 47-50 des Muster-ADV-Vertrages genau auf diesem Umstand hingewiesen.

Die landesrechtlichen Vorgaben von Berlin schreiben eine ausdrückliche Protokollierung vor, sodass dies in der Beschreibung der TOM's in der Anlage entsprechend berücksichtigt werden muss. Hier muss allerdings darauf hingewiesen werden, dass eine Protokollierung nahezu immer die Möglichkeit der Kontrolle von Arbeitnehmern beinhaltet, sodass der Auftraggeber hier rechtzeitig daran denken muss, die bei ihm zuständige Arbeitnehmervertretung wie z. B. Personal- oder Betriebsrat in den Prozess zu integrieren.

Einhaltung gesetzlicher Vorschriften des Auftraggebers

Der Auftragnehmer muss vertraglich dahingehend verpflichtet werden, dass der Auftraggeber die für ihn geltenden gesetzlichen Bestimmungen einhalten kann. Dies schließt insbesondere ein, sich der für den Auftraggeber zuständigen Aufsichtsbehörde zu „unterwerfen" (§3 Ziff. (17) des Muster ADV-Vertrages).

Dies verlangen diverse (Landes-) Gesetze. Daher ist es nicht möglich, vertraglich festzulegen, dass für den Auftragnehmer nur die bei ihm ansässige Aufsichtsbehörde zuständig ist.

In der Praxis spielt dies jedoch für den Auftragnehmer keine Rolle, da aufgrund der Aufgabenteilung die für den Auftraggeber zuständige Aufsichtsbehörde bei einer Kontrolle immer die für den Auftragnehmer zuständige Aufsichtsbehörde kontaktiert und mit der

[27] §80 SGB X gilt nur für in §35 SGB I genannte Personen/Stellen, welche Sozialdaten im Sinne von §67 Abs. 1 SGB X verarbeitet (siehe auch Kapitel 9.2 „Besonderheiten bei der Verarbeitung von Sozialdaten im Auftrag")

Prüfung des Auftragnehmers beauftragt, sodass der Auftragnehmer faktisch nur von einer Aufsichtsbehörde geprüft wird.

Datenschutzbeauftragter

Der Auftrag darf nur erteilt werden, wenn beim Auftragnehmer ein ordentlich bestellter Datenschutzbeauftragter vorhanden ist, welcher dem Auftraggeber namentlich benannt werden muss (§3 Ziff. (6)) – sofern eine Bestellpflicht besteht bzw. dies gesetzlich für eine Auftragsvergabe gefordert wird. Entsprechend §4f Abs. 1 BDSG haben öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Datenschutzbeauftragten zu bestellen, d. h., wenn die Auftragsvergabe eine automatisierte Datenverarbeitung, also eine Datenverarbeitung unter Nutzung von Computertechnologie, beinhaltet, muss ein Datenschutzbeauftragter bestellt werden.

Der Düsseldorfer Kreis veröffentlichte die Mindestanforderungen an Fachkunde und Unabhängigkeit eines Datenschutzbeauftragten[28]. Dies sind, wie es der Titel schon besagt, die Mindestanforderungen, die für eine ordnungsgemäße Bestellung unabdingbar sind. Die Erfüllung dieser Bedingungen muss dem Auftraggeber im Rahmen seiner Überzeugungsbildung nachgewiesen werden.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) veröffentlichte ein berufliches Leitbild des Datenschutzbeauftragten[29]. Darin werden z. T. Anforderungen beschrieben, die über die Ansprüche des Düsseldorfer Kreises hinausgehen. Es ist wünschenswert, wenn der Datenschutzbeauftragte des Auftragnehmers dem Berufsbild genügt; für die Auftragsvergabe ist dies jedoch keine zwingende Voraussetzung.

Mitteilung bei Verstößen

Der Auftragnehmer muss dem Auftraggeber über Missachtungen bzgl. der vertraglich vereinbarten Leistungen bzw. über datenschutzrechtliche Verstöße informieren (§3 Ziff. (7)), damit der Auftraggeber seiner gesetzlichen Verpflichtung bzgl. Information des Betroffenen bzw. Information der Aufsichtsbehörde nachkommen kann.

Hinweis bei Zweifel an der Rechtmäßigkeit einer Beauftragung

Der Auftragnehmer ist zwar nicht verpflichtet, die Rechtmäßigkeit des auftragsgemäßen Umgangs sorgfältig zu prüfen, denn dies ist die Aufgabe des Auftraggebers. Existieren jedoch Zweifel an der Rechtmäßigkeit, so ist der Auftragnehmer unverzüglich zu einem Hinweis gegenüber dem Auftraggeber verpflichtet[30]. Eine Informationspflicht des Auftragnehmers bei Zweifeln ergibt sich auch aus den nebenvertraglichen Pflichten (z. B. BGH, Urt. v. 19. Mai 2011, AZ VII ZR 24/08).

Für einen entsprechenden Hinweis darf der Auftragnehmer daher nicht warten, bis der Auftragnehmer sichere Kenntnis von der Rechtswidrigkeit hat[31]. Betrifft der Auftrag besonders sensitive Daten wie Gesundheitsdaten, so ist der Auftragnehmer zudem zu einer erhöhten Aufmerksamkeit verpflichtet[31]. Die Verantwortlichkeit des Auftraggebers bedingt, dass er bei unsicherer Rechtslage grundsätzlich die Erfüllung seiner Weisung durch den Auftragnehmer verlangen kann[32]. Der Auftragnehmer hat nur das Recht die Durchführung einer Weisung zu verweigern, wenn

---

[28] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 24./25. November 2010). [Online] 2010 [Zitiert 2014-03-31] Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?__blob=publicationFile

[29] Berufsverband der Datenschutzbeauftragten Deutschlands: Berufliches Leitbild der Datenschutzbeauftragten). [Online] 2010 [Zitiert 2014-03-31] Verfügbar unter https://www.bvdnet.de/as-berufsbild.html

[30] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 92 zu §11

[31] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 91 zu §11

[32] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 95 zu §11

- die Rechtslage eindeutig ist,
- schwere Persönlichkeitsverletzungen im Raum stehen oder
- der Auftragnehmer bei einer Durchführung das Risiko einer strafbaren Handlung auf sich nehmen würde.

§3 Abs. (15) bietet daher dem Auftragnehmer die Möglichkeit, aus seiner Sicht rechtswidrige Verarbeitungen bis zu einer Bestätigung oder Änderung des Auftrags durch den Auftraggeber auszusetzen, da allein der hinweispflichtige Zweifel an der rechtskonformen Verarbeitung den Auftragnehmer ansonsten nicht berechtigen würde, eine ggfs. rechtswidrige Verarbeitung durchzuführen.

Verpflichtung des vom Auftragnehmer eingesetzten Personals

Im Rahmen einer Auftragsdatenverarbeitung muss der Auftragnehmer vertraglich verpflichtet werden, das von ihm eingesetzte Personal auf die Einhaltung des Datengeheimnisses zu verpflichten (§3 Ziff. (5)).

Für den Auftragnehmer gelten in den seltensten Fällen die landesrechtlichen Vorschriften. Die Regel wird sein, dass es sich beim Auftragnehmer um eine nicht-öffentliche Stelle handelt, für welche das BDSG gilt. Dementsprechend muss der Auftragnehmer die Verpflichtung anhand der Vorschriften des BDSG vornehmen. Im Rahmen der Wartung wird des Öfteren auch das Fernmeldegeheimnis betroffen sein, sodass eine Verpflichtung der Mitarbeiter nach §88 TKG sinnvoll erscheint, auch wenn der Auftragnehmer nicht zwingend ein Dienstanbieter entsprechend der Definition von §3 Ziff. 6 TKG ist.

Das Gesetz gegen den unlauteren Wettbewerb (UWG) setzt in §17 den Verrat von Geschäfts- und Betriebsgeheimnissen unter Strafe. Die während der Tätigkeit für den Auftraggeber vom Auftragnehmer erlangten Patientendaten sind als derartige Geheimnisse zu werten, deren Weitergabe strafrechtlich verfolgt werden kann. Durch eine Verpflichtung des vom Auftragnehmer eingesetzten Personals auf §17 UWG wird der Verrat von Geheimnissen strafrechtlich verfolgbar, ähnlich, wie es §203 StGB vorsieht. Entsprechend den landesrechtlichen Vorgaben muss dafür Sorge getragen werden, dass der aus §203 StGB resultierende Schutz des Arztgeheimnisses beim Auftragnehmer gewahrt ist. Daher wird im Muster ADV-Vertrag die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen gefordert (§3 Ziff. (5)); eine Verpflichtung nach dem UWG ermöglicht eine strafrechtliche Verfolgung bei Verrat von Geschäftsgeheimnissen des Auftraggebers, wozu im Rahmen einer Auftragsdatenverarbeitung auch die Gesundheitsdaten gehören.

Berichtigung und Löschung von Daten

Betroffene haben grundsätzlich das Recht auf Berichtigung, Sperrung und Löschung der Daten. Im Rahmen einer Auftragsdatenverarbeitung bleibt jedoch der Auftraggeber dem jeweiligen Betroffenen gegenüber verantwortlich, sodass nur der Auftraggeber den Auftragnehmer mit der Einleitung entsprechender Maßnahmen beauftragen kann (§3 Ziff. (9)).

Nun kann es jedoch vorkommen, dass sich ein Betroffener direkt an den Auftragnehmer wendet. Hier wird vertraglich festgehalten, wie damit umzugehen ist (§3 Ziff. (9)). Da der Auftragnehmer nicht „Herr der Daten“ ist, darf er an Betroffene oder gar Dritte von sich aus keine Auskünfte geben, sondern dies muss immer vom Auftraggeber im Einzelfall entschieden und ggf. der Auftragnehmer mit der Auskunftserteilung seitens des Auftraggebers beauftragt werden (§3 Ziff. (9)).

Gesetzliche Offenbarungspflicht

Gesetzliche Offenbarungspflichten können für den Aufragnehmer beispielsweise aus

- Anzeige geplanter Straftaten wie Mord oder Totschlag, erpresserischen Menschenraub oder Geiselnahme (entsprechend §138 StGB bzw. §139 StGB)

- §34 StGB Rechtfertigender Notstand

resultieren. Weiterhin kann eine Weitergabe der Daten im Rahmen einer

- Pfändung,
- Beschlagnahme,
- Zwangsvollstreckung oder
- Insolvenz

des Auftragnehmers erfolgen. Dem Auftragnehmer ist diesbezüglich die Pflicht aufzuerlegen, dass im Falle einer drohenden, rechtlich nicht zu verhindernden Weitergabe der Daten des Auftraggebers Letzterer unverzüglich zu informieren ist.

Umgang mit Pfändung

Prinzipiell sollten beim Auftragnehmer keine Patientendaten gespeichert werden, sondern die Datenverarbeitung ausschließlich beim Auftraggeber stattfinden. In einem (zu begründenden) Einzelfall kann es entsprechend den landesrechtlichen Bestimmungen dennoch wünschenswert sein, dass Daten beim Auftragnehmer gespeichert und dort verarbeitet werden müssen.

Für diesen Fall müssen bzgl. des Umgangs bei Gefahr einer Beschlagnahme oder Pfändung der Daten des Auftragnehmers vertragliche Regelungen getroffen werden (§3 Ziff. (18)).

Beschlagnahmeschutz

Der Beschlagnahmeschutz für Patientendaten gilt entsprechend §97 StPO, wenn sich die Gegenstände bzw. Dokumente im Gewahrsam

a) des Arztes oder
b) einer Krankenanstalt, d. h. in deren Räumlichkeiten befindet oder
c) eines Dienstleisters, der für die behandelnde Person bzw. Institution personenbezogene Daten erhebt, verarbeitet oder nutzt.

Wann der Beschlagnahmeschutz bei einem Dienstleister verarbeiteter Daten sicher besteht, ist nicht eindeutig. Die Gesetzesbegründung zu Punkt c) zeigt auf, dass die Einführung der Gesundheitskarte nicht zur Verschlechterung des Patientenschutzes führen sollte, wenn der Gewahrsam an den Daten nicht mehr beim Zeugnisverweisungsberechtigten besteht, sondern bei einem Dienstleister[33].

Ohne einen rechtswirksamen Vertrag wird man jedoch wohl davon ausgehen müssen, dass bei einem Dienstleister kein Beschlagnahmeverbot gilt. Beinhaltet die Datenverarbeitung eines Dienstleisters daher einen Verstoß gegen §203 StGB, so wird aus diesem Verstoß wahrscheinlich eine rechtsunwirksame Datenauslagerung bzw. Datenverarbeitung resultieren, die mit einer Unwirksamkeit hinsichtlich des Beschlagnahmeschutzes verbunden sein wird. Daher sollte eine Bearbeitung von Patientendaten ausschließlich in der jeweiligen Institution erfolgen (§3 Ziff. 20).

Im Falle der Beauftragung von (Fern-) Wartungstätigkeiten lässt sich dieses Problem gut lösen. Moderne Maßnahmen wie ein Remote Desktop erlauben eine Fernwartung, ohne dass dabei Daten auf den Rechnern des fernwartenden Personals abgespeichert werden. Es werden lediglich Bildschirminhalte übertragen. Überträgt man die gängige Rechtsprechung aus den Filesharing-Prozessen, so wird durch diese Maßnahme keine Kopie der Patientendaten erstellt. Letztlich existieren somit auch keine Patientendaten beim Auftragnehmer, die beschlagnahmt werden könnten.

[33] Drucksache 15/1525 (2003-09) Gesetzentwurf der Fraktionen SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN: "Entwurf eines Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG). Begründung zu Artikel 30, S.167/168 [Online, zitiert am 2014-12-10]; Verfügbar unter http://dipbt.bundestag.de/doc/btd/15/015/1501525.pdf

Sinnvollerweise vereinbaren Auftraggeber und Auftragnehmer, dass der Auftragnehmer keine Patientendaten zur Speicherung in seinen Systemen anfordert und der Auftraggeber eine entsprechende Anforderung verweigert. Diese Vereinbarung erschwert sicherlich dem Auftragnehmer im Einzelfall die Fehlersuche in dem zu wartendem System, ist aber aus strafrechtlichen, nicht jedoch aus datenschutzrechtlichen Gesichtspunkten zu fordern.

Umgang mit TOM's

Da in §3 des Muster ADV-Vertrages die Pflichten des Auftragnehmers dargestellt werden, wird hier die Umsetzung und Einhaltung der vereinbarten TOM's vertraglich vereinbart (§3 Ziff. (2)). Insbesondere wird auch der Umgang mit Änderungen der TOM's beschrieben.

Datenschutzverstöße beim Auftragnehmer

Der Auftraggeber ist und bleibt im Rahmen einer Auftragsdatenverarbeitung „Herr der Daten". Dementsprechend muss er auch jederzeit über Vorkommnisse in Bezug auf den Umgang mit seinen Daten informiert werden, damit er entsprechend den gesetzlichen Bestimmungen den Betroffenen oder die für ihn zuständige Aufsichtsbehörde informieren kann. Damit er diese gesetzliche Verpflichtung einhalten kann, muss der Auftragnehmer vertraglich zur Weitergabe entsprechender Informationen verpflichtet werden (§3 Zeilen Ziff. (7) und (13)).

Auskunft durch den Auftraggeber

Der Auftraggeber muss auf Nachfrage dem Betroffenen über Art und Umfang der Verarbeitung seiner Daten informieren. Dabei ist der Auftraggeber ggfs. darauf angewiesen, dass der Auftragnehmer ihm Informationen bzgl. der von ihm durchgeführten Datenverarbeitung gibt. Um der gesetzlichen Auskunftspflicht nachzukommen, muss der Auftraggeber diese Pflicht des Auftragnehmers daher im ADV-Vertrag verankern (§3 Ziff. (13))

Zweitnutzung der Daten durch den Auftragnehmer

Verschiedene Gesetze (z. B. das Berliner Krankenhausgesetz in Verbindung mit dem Berliner Datenschutzgesetz) erlauben keine Nutzung der Daten zu anderen als zu den im ADV-Vertrag beschriebenen Zwecken. Daher muss ein explizites Verbot einer Nutzung der Daten durch den Auftragnehmer zu anderen Zwecken im Vertrag ausgesprochen werden (§3 Ziff. (19)).

Zuständige Aufsichtsbehörde

Grundsätzlich können sowohl Auftragnehmer wie auch Auftraggeber entsprechend §38 BDSG durch die zuständige Aufsichtsbehörde kontrolliert werden, obwohl bzgl. des konkreten Umgangs mit personenbezogenen Daten zunächst der Auftraggeber Adressat aufsichtsbehördlicher Maßnahmen sein dürfte. Maßnahmen entsprechend §38 Abs. 5 (= Prüfung und Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen) gegen den Auftragnehmer sind jedoch immer möglich.

Mehrere datenschutzrechtliche Landesgesetze fordern jedoch explizit, dass vertraglich geregelt wird, dass sich der Auftragnehmer der für den Auftraggeber zuständigen Aufsichtsbehörde unterwirft, so z. B. in:

- Baden-Württemberg,
- Bremen,
- Mecklenburg-Vorpommern,
- Nordrhein Westfalen,
- Sachsen-Anhalt und
- Thüringen.

Gleiches gilt für kirchenrechtliche Regelungen bzgl. datenschutzrechtlicher Anforderungen zur Auftragsdatenverarbeitung.

Literatur

1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
2) Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2010) Kontrollzuständigkeiten bei Datenverarbeitung im Auftrag. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/KontrollzustaendigkeitAufragsdatenverarbeitung.pdf?__blob=publicationFile
3) Gaulke M. (2011) Prüfung der Einhaltung der technischen und organisatorischen Maßnahmen bei Auftragsdatenverarbeitungen. DuD: 417-420
4) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
5) Münch P. (2010) Technisch-organisatorischer Datenschutz: - Leitfaden für Praktiker. 4. Auflage. Datakontext Verlag
6) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
7) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

§4 Pflichten des Auftraggebers

Alt. 1 zu Abs. 1

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

Alt. 2 zu Abs. 1

(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.

Opt. (6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

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

Kommentierung §4

§11 BDSG wie auch §80 SGB X[34] sowie die entsprechenden landes- und kirchenrechtlichen Gesetze regeln, dass der Auftraggeber datenschutzrechtlich die verantwortliche Stelle bleibt. Entsprechend können einige daraus resultierende Pflichten nicht vom Auftragnehmer übernommen werden, sondern obliegen dem Auftraggeber.

Verantwortliche Stelle

Verantwortliche Stelle im Sinne des Datenschutzrechts bleibt der Auftraggeber (§4 Ziff. 0). Desgleichen kann der Auftraggeber auch nicht andere Pflichten (z. B. aus §203 StGB resultierendes Arztgeheimnis) an den Auftragnehmer weiterreichen, sondern die Pflichten obliegen eindeutig allein dem Auftraggeber.

Daraus resultiert auch, dass der Auftraggeber für die beim Auftragnehmer stattfindende Datenverarbeitung datenschutzrechtlich verantwortlich bleibt (§4 Ziff. (3)) und dementsprechend das Verfahrensverzeichnis zu führen hat. Gleiches gilt für die Rechte des Betroffenen (§§6-8 BDSG), die der Betroffene gegenüber dem Aufragnehmer geltend machen kann. Die Verantwortlichkeit des Auftragnehmers gegenüber dem Betroffenen berührt jedoch nicht die Frage nach einer Haftung des Auftragnehmers gegenüber dem Auftraggeber im Innenverhältnis (siehe §9 bzw. entsprechende Kommentierung).

Informationspflichten des Auftraggebers

Der Gesetzgeber sieht vor (z. B. §42a BDSG), dass eine datenverarbeitende Stelle einen Betroffenen bei unrechtmäßiger Kenntniserlangung seiner Daten gegebenenfalls informieren muss. Diese Pflicht bleibt beim Auftraggeber (§4 Ziff. (4)) als für die Daten verantwortliche Stelle. Je nach erteilter Weisung gelten für den Auftraggeber neben den Pflichten aus BDSG, Landes- oder Kirchenrecht auch die Informationspflichten aus dem Telemediengesetz; daher wird hierauf ebenfalls hingewiesen.

Über den Vertrag hinausgehende Anweisungen

Erteilt der Auftraggeber dem Auftragnehmer Weisungen, welche über die vertraglich vereinbarten Leistungen hinausgehen, so kann der Auftragnehmer dem Auftraggeber die daraus resultierenden Kosten in Rechnung stellen (§4 Opt. (7)). Diese Regelung ist gesetzlich nicht gefordert, entspricht aber den Gepflogenheiten zwischen Vertragsparteien.

Literatur

1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
2) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
3) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
4) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

[34] §80 SGB X gilt nur für in §35 SGB I genannte Personen/Stellen, welche Sozialdaten im Sinne von §67 Abs. 1 SGB X verarbeitet (siehe auch Kapitel 9.2 „Besonderheiten bei der Verarbeitung von Sozialdaten im Auftrag“)

§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 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.

Opt. (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.

Opt. (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.

Kommentierung §5

Die Löschung der Daten, welche der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten in seinen eigenen Systemen speichern musste, nach Abschluss der Arbeiten durch den Auftragnehmer ist gesetzlich vorgeschrieben (z. B. §80 Abs. 2 Ziff. 10 SGB X). Daher muss die Löschung der Daten unabhängig vom Weisungsrecht des Auftraggebers vertraglich abgebildet werden (§5 Ziff. (1)).

Dabei ist der Nachweis der Erbringung der vertraglich geschuldeten Leistungen seitens des Auftragnehmers ggfs. über das Vertragsende hinaus aufzubewahren. Hier nur der Hinweis, dass Bestell- und Auftragsunterlagen eine gesetzliche Aufbewahrungsfrist von derzeit 6 Jahren aufweisen, EDV-Unterlagen, wenn sie zum Verständnis der Buchführung erforderlich sind, 10 Jahre aufbewahrt werden müssen. Daher wird im Vertrag darauf hingewiesen, dass derartige Unterlagen vom Auftragnehmer nicht gelöscht werden müssen (§5 Ziff. (2)).

Literatur

1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
2) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
3) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
4) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

§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.

Kommentierung §6

Der Gesetzgeber fordert vom Auftraggeber, dass er sich vor und nach Vertragsabschluss sowie während der Vertragslaufzeit von der Einhaltung der vertraglich vereinbarten Bedingungen, insbesondere der TOM's überzeugt. Daher muss der Auftraggeber vor Abschluss des ADV-Vertrages und danach in regelmäßigen Abständen die Einhaltung der im ADV-Vertrag vereinbarten Pflichten des Auftragnehmers prüfen[35] und das Ergebnis der Prüfung dokumentieren (§4 Ziff.(1))[36]. Entsprechend $43 Abs. 1 Nr. 2b kann die Aufsichtsbehörde ein Bußgeld verhängen, wenn der Nachweis einer erfolgten Erstkontrolle vom Auftraggeber nicht erbracht werden kann. Daher sollte die Dokumentationspflicht auch entsprechend gelebt werden.

Bei Fehlern oder Unregelmäßigkeiten ist der Auftragnehmer vom Auftraggeber unverzüglich[37] zu informieren (§4 Ziff.(3)), damit der Auftragnehmer diese beseitigen kann. Da der Auftraggeber verantwortlich für die beim Auftragnehmer durchgeführte Datenverarbeitung ist, liegt die Beseitigung festgestellter Mängel im ureigenen Interesse des Auftraggebers.

Um die gesetzlich geforderten Prüfungen zu ermöglichen, muss der Auftragnehmer vertraglich dazu verpflichtet werden, diese Prüfungen zu unterstützen (§6 Ziff.(3)). Ohne eine vertraglich vereinbarte Unterstützungspflicht des Auftragnehmers ist der Auftraggeber ggfs. nicht in der Lage, die gesetzlich geforderten Kontrollen durchzuführen. Daher hat der Gesetzgeber diese Pflicht zur Regelung der Duldungs- und Mitwirkungspflichten des Auftragnehmers in §11 Abs. 2 Ziff. 7 vorgeschrieben.

Dabei muss dem Auftraggeber freigestellt bleiben, wie er zu der Überzeugungsbildung kommt. Eine „Kontrolle nur nach vorheriger Abstimmung ohne Störungen des Betriebsablaufs" schränkt die Kontrollmöglichkeiten zu stark ein; insbesondere nach einem Datenschutzvorfall kann eine unangekündigte Kontrolle unabdingbar notwendig sein, da hierbei ein Umstand vorliegt, der ggfs. eine Nichteinhaltung der vereinbarten Pflichten durch den Auftragnehmer darlegte. Eine Vorankündigung zu einer Kontrolle kann in diesem Fall einen Überzeugungsprozess beim Auftraggeber nachhaltig verhindern, sodass eine unangekündigte Kontrolle in diesem Fall nicht ausgeschlossen werden kann (§6 Ziff. (2)).

Literatur

1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
2) Bergt M. (2013) Vertragsgestaltung und Kontrolle bei Auftragsdatenverarbeitung. in Jürgen Taeger (Hrsg.) Law as a Service (LaaS) - Recht im Internet- und Cloud-Zeitalter (Band 1). Oldenburger Verlag für Wirtschaft, Informatik und Recht
3) Bierekoven C. (2012) Aktuelle Entwicklungen zur Auftragsdatenverarbeitung - Präzisierte Anforderungen der Datenschutzaufsichtsbehörden. ITRB: 280-282
4) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691

[35] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit veröffentlichte in seinem Wiki Hinweise zur Prüfung: Checkliste Datenverarbeitung im Auftrag [Online] 2013 [Zitiert 2014-03-31] Verfügbar unter http://www.bfdi.bund.de/bfdi_wiki/index.php/Checkliste_Datenverarbeitung_im_Auftrag bzw. Checkliste Datenverarbeitung Wartung [Online] 2013 [Zitiert 2014-03-31] Verfügbar unter http://www.bfdi.bund.de/bfdi_wiki/index.php/Checkliste_Datenverarbeitung_Wartung

[36] Hier ist zumindest die Textform entsprechend §126b BGB erforderlich

[37] siehe §121 Abs. 1 BGB: „ohne schuldhaftes Zögern (unverzüglich)"

5) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
6) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

§7 Unterauftragnehmer

Alt 1 von Abs. 1

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

Alt 2 von Abs. 1

(1) Die Weitergabe von Aufträgen der im Hauptvertrag konkretisierten Tätigkeiten an Unterauftragnehmer durch den Auftragnehmer bedarf der schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer hat Unterauftragnehmer nach deren Eignung sorgfältig auszuwählen.

(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.

Alt. 1 von Abs. 3

(3) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

Alt. 2 von Abs. 3

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Leistungsteile werden unter Einschaltung eines Unterauftragnehmers durchgeführt, nämlich

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen

Alt. 3 von Abs. 3

(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 den in diesem ADV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers.

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.

(5) 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.

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.

Opt. (6) Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner Pflicht zur Auftragskontrolle konzernangehörige Unternehmen mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies durch den Auftraggeber vor Beginn der Verarbeitung oder Nutzung genehmigen lässt.

Alt 1 von Opt. Abs. 7

(7) Unter-Unterauftragsverhältnisse sind ohne explizite Genehmigung durch den Auftraggeber nicht erlaubt.

Alt 2 von Opt. Abs. 7

(7) Unter-Unterauftragsverhältnisse sind analog den Vorgaben zu Unterauftragsverhältnissen datenschutzrechtlich zu gestalten.

Opt. (8) 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.

Kommentierung §7

Mitunter kann ein Hersteller alleine den ordnungsgemäßen Betrieb des verkauften Produktes nicht gewährleisten. In diesen Fällen kann es notwendig sein, dass der Auftragnehmer Unterauftragnehmer beauftragt.

Unterauftragnehmer sind alle, die nicht beim Auftragnehmer selbst beschäftigt sind bzw. nicht in einer Beziehung als Leiharbeitnehmer zum Auftragnehmer z. B. im Rahmen einer Arbeitnehmerüberlassung stehen. So kann beispielsweise eine Konzerntochter, die von einer anderen Konzerntochter beauftragt wird, als Unterauftragnehmer anzusehen sein.

Die bestehenden datenschutzrechtlichen Regelungen lassen diese Unterauftragnehmerschaft ausdrücklich zu, verlangen aber, dass diese Verhältnisse im ADV-Vertrag geregelt werden.

Unter dem Aspekt, dass der Gesetzgeber fordert, dass bei einem ADV-Vertrag der Auftraggeber stets „Herr der Daten“ bleibt, muss natürlich der Auftraggeber zu jedem Zeitpunkt wissen, wer Zugriff auf seine personenbezogenen oder personenbeziehbaren Daten hat. Dies beinhaltet, dass die Unterauftragnehmerschaft vom Auftraggeber genehmigt werden muss.

Es ist zweifelhaft, ob eine generelle Erlaubnis des Auftraggebers zu einer beliebigen Beauftragung von Unterauftragnehmern durch den Auftragnehmer rechtlich zulässig ist, da in einem solchen Fall der Auftraggeber nicht mehr bestimmen kann, wer auf die zu schützenden Daten zugreift und somit seine „Herrschaft“ verliert; der Vollständigkeit halber wurde die Option trotzdem aufgeführt (§7 Alt. 1 von Abs. 3). Zudem widerspricht eine derartige Regelung verschiedenen rechtlichen Vorgaben. Um einen bundesweit gültigen Muster ADV-Vertrag abbilden zu können, muss daher im Vertrag festgehalten werden, dass Unterauftragsverhältnisse im Einzelfall vom Auftraggeber zu genehmigen sind.

Idealerweise werden daher bei Vertragsabschluss die Unterauftragnehmer im Vertrag aufgeführt. Natürlich können sich die Unterauftragnehmer während eines längerfristigen Auftrags, wie es beispielsweise bei der Wartung eines medizinischen Informationssystems zu erwarten ist, ändern. In diesem Fall beauftragt der Auftragnehmer nach Rücksprache und schriftlicher Genehmigung durch den Auftraggeber den neuen Unterauftragnehmer.

Dabei ist es statthaft, die Zustimmung des Auftraggebers vertraglich anhand von definierten Kriterien zu vereinbaren. D. h., der Auftraggeber wird vertraglich verpflichtet dem Unterauftragsverhältnis zuzustimmen, wenn bestimmte Kriterien eingehalten werden. Diese Kriterien dürfen jedoch nicht willkürlich sein, sondern müssen für die ordnungsgemäße Abwicklung des Auftrags zwingend Voraussetzung sein.

Unteraufträge sollten ausdrücklich festhalten, dass die Kontrollrechte des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten (§7 Abs. (4)), da der Auftraggeber sonst seiner gesetzlich vorgeschriebene Verantwortung nicht nachkommen kann[38].

Auftragsdatenverarbeitung außerhalb des EWR

Gerade im Bereich der medizinischen Informationssysteme existieren neben einigen Konzernen auch viele kleine mittelständische Unternehmen mit einer Mitarbeiterzahl, welche einen 24-Stunden-Support in einer 7-Tage-Woche, wie es im Krankenhaus mitunter notwendig ist, nur anbieten können, indem Mitarbeiter in anderen Ländern eingesetzt werden. Hierbei ist zu beachten, dass – je nachdem in welchem Land die mit dem Support oder der Fernwartung beauftragten Mitarbeiter sitzen – eine Auftragsdatenverarbeitung mit einem deutschen Standardvertrag alleine nicht zulässig ist.

[38] Petri T. (2014) in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 76 zu §11

Innerhalb der Europäischen Union oder des EWR (die Länder der EU sowie Island, Liechtenstein und Norwegen) existiert ein vergleichbar hohes Datenschutzniveau, sodass ein ADV-Vertrag entsprechend deutschem Recht abgeschlossen wird. Eine Beauftragung von Auftragnehmern in Ländern, denen die europäische Kommission bereits ein angemessenes Datenschutzniveau attestiert hat, ist ebenfalls problemlos möglich; die Liste der Länder ist online unter http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm verfügbar.

Gemäß Art. 25 der EG-Datenschutzrichtlinie und §4b Abs. 2 S. 2 des BDSG ist stets die Sicherstellung eines angemessenen Datenschutzniveaus beim Datenempfänger anzustreben. Die europäische Kommission stellte daher sogenannte „Standardvertragsklauseln“ bereit, welche beim Einsatz eines Auftragsdatenverarbeiters in einem sogenannten Drittland (= Land ohne hinreichendes Datenschutzniveau) verwendet werden müssen, wenn unter dem Aspekt der Auftragsdatenverarbeitung ein Auftragnehmer eines derartigen Landes von einem Auftraggeber mit Sitz in der EU beauftragt werden soll. Diese Vertragsvorgaben ergänzen und präzisieren die Vertragsbedingungen über die eigentliche Leistungserbringung hinsichtlich der datenschutzrechtlich geforderten Mindeststandards. Die Rechte und Pflichten der Parteien werden geregelt und müssen unverändert übernommen werden.

Entsprechend §4c BDSG sind auch Ausnahmen möglich, in denen personenbezogene Daten in ein Drittland ohne angemessenes Datenschutzniveau transportiert werden dürfen. Im Rahmen der hier betrachteten Fragestellung (Beauftragung eines Auftragnehmers durch ein deutsches Krankenhaus für Outsourcingmaßnahmen) kommt als Ausnahme lediglich die (informierte) Einwilligung aller Betroffenen in Betracht. Aus praktischen Gründen kommt diese Möglichkeit letztlich nicht in Betracht, sodass nur ein Vertrag unter Nutzung der EU-Standardvertragsklauseln in Frage kommt.

Seit dem 15.5.2010 müssen die neuen EU-Standardvertragsklauseln genutzt werden. Die zuvor veröffentlichten Klauseln dürfen nicht mehr verwendet werden, jedoch behalten bereits bestehende Vereinbarungen ihre Gültigkeit, solange weiterhin in diesem Verhältnis Daten übermittelt werden und die Übermittlung und Verarbeitung keiner Änderung unterliegt.

Literatur

1) Artikel-29-Datenschutzgruppe. (2009) Stellungnahme 3/2009 über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter). [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_de.pdf
2) Artikel-29-Datenschutzgruppe. (2010) Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG. [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf
3) Bayerisches Landesamt für Datenschutzaufsicht. (2012) Die Anforderungen des §11 BDSG müssen auch bei der Weitergabe von Daten an Auftragsdatenverarbeiter in Drittstaaten eingehalten werden. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm

4) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
5) Düsseldorfer Kreis. (2007) Internationaler Datenverkehr. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/April07IntDatenverkehr.pdf?__blob=publicationFile
6) Düsseldorfer Kreis. (2010) Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile
7) Düsseldorfer Kreis. (2013) Datenübermittlung in Drittstaaten. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/12092013DatenuebermittlungInDrittstaaten.pdf?__blob=publicationFile
8) Eckhardt J. (2013) Auftragsdatenverarbeitung - Gestaltungsmöglichkeiten und Fallstricke. DuD: 585-591
9) Erd R. (2011) Auftragsdatenverarbeitung in sicheren Drittstaaten. DuD: 275-278
10) Eul H, Eul P. (2011) Datenschutz International: Ein Praxisleitfaden für die Übermittlung von Kunden-, Mitarbeiter- und Lieferantendaten. 1. Auflage. Datakontext Verlag
11) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
12) Kremer S. (2014) Leistungsketten in der Auftragsdatenverarbeitung - Anforderungen an die Einbeziehung von (Unter-)Unterauftragnehmern nach dem BDSG. ITRB: 60-66
13) Lensdorf L. (2010) Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern - Besonderheiten der neuen EU-Standardvertragsklauseln. CR: 735-741
14) Moos F. (2010) Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010 - Die wesentlichen Neuerungen und Kritikpunkte im Überblick. CR: 281-286
15) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
16) Schmidl M, Krone D. (2010) Standardvertragsklauseln als Basis intra-europäischer Auftragsdatenverarbeitung. DuD: 838-843
17) Scholz M, Lutz H. (2011) Standardvertragsklauseln für Auftragsverarbeiter und §11 BDSG - Ein Plädoyer für die Unanwendbarkeit der §§11 Abs. 2, 43 Abs. 1 Nr. 2b) BDSG auf die Auftragsverarbeitung außerhalb des EWR. CR: 424-428
18) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand
19) Voigt P. (2012) Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland? ZD: 546-550
20) Weber M, Voigt P. (2011) Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. ZD: 74-78

§8 Individualvertragliche Ergänzung

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

Opt. §9 Haftung

> ***Bemerkung:*** *Haftungsfragen sollten nur im Hauptvertrag geregelt werden. Eine Regelung im ADV-Vertrag ist daher nur erforderlich, wenn eine entsprechende Regelung im Hauptvertrag nicht vorgenommen wurde und die Vertragsparteien diese Regelung im ADV-Vertrag unbedingt vereinbaren wollen.*

(1) Der Auftragnehmer schließt seine Haftung für leicht fahrlässige Pflichtverletzungen aus, sofern diese keine vertragswesentlichen Pflichten, Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Garantien betreffen oder Ansprüche nach dem Produkthaftungsgesetz berührt sind. Gleiches gilt für Pflichtverletzungen seiner Erfüllungsgehilfen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§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.

(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.

Opt. (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.
- Anlage 3: EU-Standardvertragsklauseln zur Beauftragung von Unterauftragsverhältnissen

Kommentierung §8 - 12

Haftung vs. Vertragsstrafe

Die Vertragsstrafe kann bis zur Grenze der Sittenwidrigkeit gemäß §138 BGB beziffert werden[39]. Daher ist eine richtige Bezifferung des Schadens eine unumgängliche Anforderung, damit eine entsprechende Vertragsstrafe eingefordert werden kann. Um vertraglich diese Summe vereinbaren zu können, muss diese Schadenssumme im Vorhinein abgeschätzt werden, was oftmals nicht möglich ist.

Oftmals besteht im Rahmen einer Auftragsverarbeitung für den Auftraggeber der größte Schaden in einem Imageverlust. Dieser Schaden, der unzweifelhaft vorhanden ist, ist monetär im Falle des Eintritts nur schwer bezifferbar und im Vorfeld realistisch kaum einschätzbar.

§437 BGB geht vom Grundgedanken aus, dass Haftung und Gewährleistung nebeneinander bestehende Rechte sind und sich wechselseitig ergänzen. Ein genereller vertraglicher Ausschluss eines Haftungsanspruchs des Auftragnehmers gegenüber dem Auftraggeber ist daher nicht möglich. Entsprechend BGB sind insbesondere folgende Beschränkungen der Haftung nicht möglich:

- arglistiges Verhalten (§444 BGB),
- das Bestehen von Garantien (§444 BGB),
- die Haftung für Schäden aus der Verletzung von Leben, Körper und Gesundheit (§309 Nr. 7a BGB),
- die Haftung für grobes Verschulden (§309 Nr. 7b BGB) sowie
- Ansprüche aus Produkthaftungsgesetz (§14 ProdHaftG).

Der Auftragnehmer muss für alle wichtigen Pflichtverletzungen und Leistungsstörungen aufkommen und kann die Haftung nicht ausschließen. Zulässig ist daher lediglich eine Einschränkung der Haftung entsprechend Ziff. 0 in §9. Die Frage, ob die Aufnahme einer solchen Klausel in ein Vertragswerk sinnvoll ist, müssen die Vertragsparteien untereinander absprechen.

Individualvertragliche Ergänzung

Aufgrund von §273 BGB besteht ggfs. die Möglichkeit, dass der Auftragnehmer Daten des Auftraggebers nicht löscht oder an den Auftraggeber zurückgibt. Zum Schutz der Patientendaten verzichtet der Auftragnehmer durch eine individualvertragliche Vereinbarung auf diese Möglichkeit (§8).

Aufgrund der §§310 Abs. 1 S. 1 und 2, 307, 309 Nr. 2 lit. b BGB muss dieser Umstand ggfs. individualvertraglich vereinbart werden, da evtl. entsprechend formulierte Bestimmungen in Allgemeinen Geschäftsbedingungen nicht gültig sein können.

Literatur

1) Eckhardt J. (2013) Auftragsdatenverarbeitung - Gestaltungsmöglichkeiten und Fallstricke. DuD: 585-591
2) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691

[39] Palandt. Bürgerliches Gesetzbuch. 72. Auflage 2013. Verlag C.H.Beck: §138 Rn 102 mit Verweis auf §339 Rn. 2

3) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
4) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

Anlage 1 zum ADV-Vertrag: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Kommentierung Anhang 1

Damit der Auftraggeber die Kontrolle über seine Daten wahrnehmen kann, muss er wissen, wer wann zu welchem Zweck auf welche Daten von wo aus zugreift. Dementsprechend muss der Auftraggeber bzgl. vom Auftragnehmer eingesetzten Unterauftragnehmern nicht nur deren Namen wissen, sondern auch welche Aufgaben diese von wo aus wahrnehmen.

Literatur

Siehe Seite 67

Anlage 2 zum ADV-Vertrag: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

1) Zutrittskontrolle

☐ Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Zutrittskontrolle.
☐ Es existieren folgende Maßnahmen zur Zutrittskontrolle:

1) …
2) …
3) …

2) Zugangskontrolle

☐ Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Zugangskontrolle.
☐ Es existieren folgende Maßnahmen zur Zugangskontrolle:

1) …
2) …
3) …

3) Zugriffskontrolle

☐ Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Zugriffskontrolle.
☐ Es existieren folgende Maßnahmen zur Zugriffskontrolle:

1) …
2) …
3) …

4) Weitergabekontrolle

☐ Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Weitergabekontrolle.
☐ Es existieren folgende Maßnahmen zur Weitergabekontrolle:

1) …
2) …
3) …

5) Eingabekontrolle

☐ Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Eingabekontrolle.
☐ Es existieren folgende Maßnahmen zur Eingabekontrolle:

1) …
2) …
3) …

6) Auftragskontrolle

☐ Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Auftragskontrolle.
☐ Es existieren folgende Maßnahmen zur Auftragskontrolle:

1) …
2) …
3) …

7) Verfügbarkeitskontrolle

☐ Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle.
☐ Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

1) …
2) …
3) …

8) Trennungskontrolle

☐ Es sind keine Maßnahmen zur Trennungskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Trennungskontrolle.
☐ Es existieren folgende Maßnahmen zur Trennungskontrolle:

1) …
2) …
3) …

Kommentierung Anhang 2

1) Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden; Beispiele sind:

- Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte (zu beachten: §6c BDSG)
- (Kontrollierte) Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung Alarmanlage, Video- / Fernsehmonitor (zu beachten: §6b BDSG)

2) Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen; Beispiele sind:

- Kennwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro Benutzer
- Verschlüsselung von Datenträgern (entsprechend dem Stand der Technik)

3) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können; Beispiele sind:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Auswertungen
- Kenntnisnahme
- Veränderung
- Löschung
- Verschlüsselungsverfahren entsprechend dem Stand der Technik

Hinweis: Bei Online-Zugriffen des Auftraggebers ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.

Verschiedene landesrechtliche Vorgaben verlangen, dass ein Wartungsvorgang nur mit Wissen und Wollen des Auftraggebers erfolgen darf. D. h. der Auftraggeber muss jeden einzelnen Wartungsvorgang veranlassen.

4) Weitergabekontrolle

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

Bitte daran denken, dass die landesrechtlichen Vorgaben von Berlin eine Protokollierung vorschreiben. Desgleichen verbietet das Berliner Landesrecht eine Datenübermittlung durch den Auftragnehmer, was in den TOM's ebenfalls berücksichtigt werden muss.

Beispiele für die Weitergabekontrolle sind:

- Identifizierung und Authentifizierung
- Tunnelverbindung (= Virtual Private Network); Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle
- Elektronische Signatur
- Protokollierung
- Transportsicherung
- Verschlüsselung entsprechend dem Stand der Technik

5) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind; ein Beispiel hierzu ist:

- Protokollierungs- und Protokollauswertungssysteme

Bitte daran denken, dass die landesrechtlichen Vorgaben von Berlin eine Protokollierung vorschreiben.

6) Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Insbesondere sind hierbei die technischen und/oder organisatorischen Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer zu regeln.

Beispiele sind:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung

7) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: Beispiele sind insbesondere:

- Backup-Verfahren: Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort für Backup
- Spiegeln von Festplatten, z. B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Virenschutz / Firewall
- Notfallplan

8) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können; Beispiele für eine Trennungskontrolle sind:

- (Interne) Mandantenfähigkeit

- Zweckbindung
- Funktionstrennung /Produktion / Test

Literatur

Anlage 3: EU-STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur):
.....
Anschrift:
.....
Tel.: ..... Fax .....
E-Mail: .....
Weitere Angaben zur Identifizierung der Organisation
.....
.....

(„Daten**exporteur**“)

und

Bezeichnung der Organisation (Datenimporteur):
.....
Anschrift:
.....
Tel.: ..... Fax .....
E-Mail: .....
Weitere Angaben zur Identifizierung der Organisation:
.....
.....

(„Daten**importeur**“)

(die „Partei“, wenn eine dieser Organisationen gemeint ist, die „Parteien“, wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1 Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ([40]);

[40] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

b) der „Datenexporteur“ ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur“ ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter“ ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2 Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3 Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4 Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten

Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5 Pflichten des Datenimporteurs ([41])

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

[41] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über
   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
   ii) jeden zufälligen oder unberechtigten Zugang und
   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6 Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.
Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7 Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder
b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8 Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9 Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist,
nämlich: .....

Klausel 10 Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11 Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss ([42]). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

[42] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich:

.....

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12 Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Für den Datenexporteur:
Name (ausgeschrieben): .....
Funktion: .....
Anschrift: .....
Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Für den Datenimporteur:
Name (ausgeschrieben): .....
Funktion: .....
Anschrift: .....
Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:

Unterschrift .....

(Stempel der Organisation)

Anhang 1 zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.
Die Mitgliedstaaten können entsprechend den nationalen Verfahren Zusatzangaben, die in diesem Anhang enthalten sein müssen, ergänzen.

Datenexporteur
Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):
.....
.....
.....

Datenimporteur
Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):
.....
.....
.....

Betroffene Personen
Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):
.....
.....
.....

Kategorien von Daten
Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):
.....
.....
.....

Besondere Datenkategorien (falls zutreffend)
Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):
.....
.....
.....

Verarbeitung
Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):
.....

.....
.....

DATENEXPORTEUR
Name: .....
Unterschrift des/der Bevollmächtigten: …….....
DATENIMPORTEUR
Name: .....
Unterschrift des/der Bevollmächtigten: .....

Anhang 2 zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

.....

.....

.....

.....

BEISPIEL FÜR EINE ENTSCHÄDIGUNGSKLAUSEL (FAKULTATIV)

Haftung

Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist.

Die Entschädigung ist abhängig davon, dass

a) der Datenexporteur den Datenimporteur unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und
b) der Datenimporteur die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten ([43]).

[43] Der Absatz über die Haftung ist fakultativ.

Literatur zu Anhang 3

1) Artikel-29-Datenschutzgruppe. (2009) Stellungnahme 3/2009 über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter). [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_de.pdf
2) Artikel-29-Datenschutzgruppe. (2010) Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG. [Online, zitiert am 2014-08-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf
3) Bayerisches Landesamt für Datenschutzaufsicht. (2012) Die Anforderungen des §11 BDSG müssen auch bei der Weitergabe von Daten an Auftragsdatenverarbeiter in Drittstaaten eingehalten werden. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm
4) Düsseldorfer Kreis. (2010) Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile
5) Düsseldorfer Kreis. (2013) Datenübermittlung in Drittstaaten. [Online, zitiert am 2014-08-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/12092013DatenuebermittlungInDrittstaaten.pdf?__blob=publicationFile
6) Erd R. (2011) Auftragsdatenverarbeitung in sicheren Drittstaaten. DuD: 275-278
7) Eul H, Eul P. (2011) Datenschutz International: Ein Praxisleitfaden für die Übermittlung von Kunden-, Mitarbeiter- und Lieferantendaten. 1. Auflage. Datakontext Verlag
8) Lensdorf L. (2010) Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern - Besonderheiten der neuen EU-Standardvertragsklauseln. CR: 735-741
9) Moos F. (2010) Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010 - Die wesentlichen Neuerungen und Kritikpunkte im Überblick. CR: 281-286
10) Schmidl M, Krone D. (2010) Standardvertragsklauseln als Basis intra-europäischer Auftragsdatenverarbeitung. DuD: 838-843
11) Scholz M, Lutz H. (2011) Standardvertragsklauseln für Auftragsverarbeiter und §11 BDSG - Ein Plädoyer für die Unanwendbarkeit der §§11 Abs. 2, 43 Abs. 1 Nr. 2b) BDSG auf die Auftragsverarbeitung außerhalb des EWR. CR: 424-428
12) Voigt P. (2012) Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland? ZD: 546-550
13) Weber M, Voigt P. (2011) Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. ZD: 74-78

Abkürzungsverzeichnis

ADV	Auftragsdatenverarbeitung
Alt.	Alternative
Art.	Artikel
BayKHG	Bayerisches Krankenhausgesetz
BbgDSG	Brandenburgisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BO	Berufsordnung
BremKHDSG	Bremisches Krankenhausdatenschutzgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands
bvitg	Bundesverband Gesundheits-IT
DSG-LSA	Datenschutzgesetz Sachsen-Anhalt
EG	Europäische Gemeinschaft
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GDD	Gesellschaft für Datenschutz und Datensicherheit
GDSG	Gesundheitsdatenschutzgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie
HDSG	Hessisches Datenschutzgesetz
HKHG	Hessisches Krankenhausgesetz
HmbKHG	Hamburgisches Krankenhausgesetz
LKG	Landeskrankenhausgesetz
LKHG	Landeskrankenhausgesetz
Opt.	Optional
ProdHaftG	Gesetz über die Haftung für fehlerhafte Produkte
SächsKHG	Sächsisches Krankenhausgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
ThürKHG	Thüringer Krankenhausgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOMs	technisch-organisatorische Maßnahmen
UWG	Gesetzes gegen den unlauteren Wettbewerb