Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen

Aktualisierte, der DS-GVO angepasste zweite Version, Stand 14.06. 2017

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“

Deutsche Krankenhausgesellschaft e. V.

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

Version 2.0
Stand der Bearbeitung: 14. 06.2017

Autoren (alphabetisch)

Ina Haag	Deutsche Krankenhausgesellschaft e.V.
Andrea Hauser	Deutsche Krankenhausgesellschaft e.V.
Christoph Isele	Cerner Deutschland GmbH
Pierre Kaufmann	AGFA Healthcare GmbH
David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Lukas Mempel	Sana Kliniken AG
Christoph Nahrstedt	Nuance Communications, Inc.
Jan Neuhaus	Deutsche Krankenhausgesellschaft e.V.
Nikolaus Schrenk	Kliniken des Bezirks Oberbayern
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Kanzlei Spyra
Barbara Stöferle	dsm-s GmbH

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch 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 vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie 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!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Inhaltsverzeichnis

Vorwort zur zweiten Auflage

Mit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung am 24. Mai 2016 und deren Wirksamwerden am 25. Mai 2018 gelten ab diesem Datum nur noch die Regelungen der europäischen Datenschutz-Grundverordnung (DS-GVO) hinsichtlich der Auftragsverarbeitung (AV). Die Auftragsverarbeitung ist zudem in der DS-GVO abschließend geregelt, sodass kein nationaler Gesetzgeber innerhalb der Europäischen Union weitere Regelungen hinzufügen oder bestehende Regelungen ändern bzw. für ungültig erklären darf.

Somit sind ab dem 25. Mai 2018 deutsche Spezial-Regelungen hinsichtlich der Auftragsverarbeitung, wie sie beispielsweise in § 80 SGB X oder in einzelnen Landesgesetzen (z.B. Krankenhausgesetzen der Länder) zu finden sind, grundsätzlich ungültig und stellen keine gültigen rechtlichen Anforderungen dar; der nationale Gesetzgeber kann bzgl. der Verarbeitung von Gesundheitsdaten zwar entsprechend den Vorgaben von Art. 9 Abs. 4 DS-GVO die Auftragsverarbeitung erlauben oder auch verbieten, hat jedoch an den Modalitäten der Auftragsverarbeitung selbst nichts geändert[1].

Auch die Anforderungen an die datenschutzrechtlichen Inhalte eines Auftragsverarbeitungs-Vertrages (AV-Vertrag) sind in der DS-GVO abschließend geregelt. Diese Anforderungen entsprechen weitestgehend dem jetzigen deutschen Recht, jedoch gibt es einige Abweichungen, die bei zukünftigen Vertragsschlüssen zu beachten sind. Die Regelungen der DS-GVO gelten aber auch für alle schon vorhandenen und noch laufenden Verträge, so dass alle diese Verträge auf Konformität zu den Anforderungen der DS-GVO geprüft und ggfs. angepasst werden müssen. Die Arbeitsgruppe veröffentlichte zu diesem Thema eine entsprechende Ausarbeitung[2].

Besonderheiten des Gesundheitswesens

Auch wenn die datenschutzrechtlichen Vorgaben bzgl. einer Auftragsverarbeitung in der DS-GVO abschließend geregelt werden, bleiben viele Fragestellungen aus dem Bereich der Gesundheitsversorgung offen, auf die eine Antwort gefunden werden muss. Hierzu gehören insbesondere Auslegungen und ggf. Regelungen zu Themen wie

- Umgang mit Zurückbehaltungsrecht
- Schadensersatz- und Haftungsfragen
- Umgang mit den Informationspflichten
- Wünsche bzgl. einer Zweckänderung durch den Auftragnehmer, z. B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung
- Fragen zu Sozialdaten
- Umgang mit Datenverarbeitung außerhalb EU/EWR, d. h. auch Umgang mit EU-Standardvertragsklausen.

[1] Drucksache 110/17: Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU). [Online, zitiert am 2017-02-25]; Verfügbar unter http://dipbt.bundestag.de/dip21/brd/2017/0110-17.pdf

[2] Siehe URL … (nach Veröffentlichung)

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

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

müssen also – je nach vertraglicher Ausgestaltung – ggf. bedacht werden.

Bildung einer Arbeitsgruppe

Um diese Fragen zu bearbeiten, fand sich eine 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)
- Deutsche Krankenhausgesellschaft e.V. (DKG)
- Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)

zusammen, die sich des Themas annahm und einen kommentierten Muster-Vertrag für die Auftragsverarbeitung erstellte. Allen Beteiligten war bewusst, dass es nicht „den“ AV-Vertrag geben kann. Der erarbeitete AV-Vertrag stellt ein Muster dar, das die wesentlichen Vertragsinhalte abhandelt, aber keinen Anspruch auf Vollständigkeit erhebt.

Da momentan noch nicht absehbar ist, wann die Gesetzgeber die Spezial-Regelungen an die DS-GVO anpassen werden, stellt diese Auflage eine Version dar, die der DS-GVO entspricht.

Es bleibt den jeweiligen Nutzern des Vertrages vorbehalten, die Regelungsgegenstände den spezifischen Anforderungen anzupassen. 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.

Einführung zum Thema Auftragsverarbeitung

1 Allgemeines

1.1 Privilegierte Form

Die Auftragsverarbeitung ist auch unter der DS-GVO weiterhin eine „privilegierte“ Form der Verarbeitung, für die der europäische Gesetzgeber vertragsrechtliche Anforderungen (Art. 28 DS-GVO) aufstellt[3]. Aufgrund der gesetzlich vorgeschriebenen vertragsrechtlichen Gestaltung bleibt der Auftraggeber datenschutzrechtlich verantwortlich[4] (in der DS-GVO entsprechend auch als „Verantwortlicher“ bezeichnet). Als "privilegiert" wird diese Form der Datenverarbeitung deswegen angesehen, weil es sich hierbei nicht um eine datenschutzrechtliche Übermittlung der Daten handelt und weder eine gesetzliche Erlaubnis noch eine Einwilligung durch die Betroffenen zur Verarbeitung der Daten durch einen externen Dienstleister (Auftragnehmer, in der DS-GVO als Auftragsverarbeiter bezeichnet) benötigt werden.

1.2 Typische Merkmale einer AV

Eine Auftragsverarbeitung kann 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 Auftragsverarbeitungen sind:

- Es fehlt eine Entscheidungsbefugnis des Auftragnehmers hinsichtlich der Zwecke und Mittel der Verarbeitung.
- Es wurde vertraglich ausgeschlossen, dass der Auftragnehmer Daten zu eigenen 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 im eigenen Namen auf.

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, so dass

[3] siehe hierzu auch die begleitende Ausarbeitung „Umgang mit Altverträgen bzgl. Auftragsverarbeitung („ADV-Verträge“)“. Online, zitiert am 2017-06-14; Verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/adv_altvertraege.php

[4] siehe hierzu bspw. auch Martini M. Art. 28. Rn. 20 in Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag 1. Auflage. ISBN 978-3-406-69570-4

sowohl Auftragnehmer als auch Auftraggeber dafür Sorge tragen müssen, dass ein AV-Vertrag abgeschlossen wird, wenn eine Auftragsverarbeitung vorliegt.

1.3 Typische Beispiele einer AV

Typische Beispiele für eine Auftragsverarbeitung durch externe Dienstleister sind etwa folgende:

- 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.

2 Einordnung des AV-Vertrages in Gesamtregelwerke

2.1 Mögliche Vertragsgestaltungen

Grundsätzlich gelten für den AV-Vertrag die gleichen Voraussetzungen wie für Verträge allgemein. Demnach muss ein entsprechender Vertrag auch die Vertragsbestandteile enthalten, welche die Leistungsbeziehung zwischen den Parteien generell regelt. Hierbei handelt es sich etwa um

- die genaue Definition der zu erbringenden Leistung/(en)/Tätigkeiten,
- Vergütung/Preis,
- Haftungsfragen, usw.

Zusätzlich sind jedoch im Falle einer Verarbeitung personenbezogener Daten im Auftrag zwingend weitere Regelungen zu treffen. In welcher Form die genannten Vertragsbestandteile geregelt werden, ist frei gestaltbar. Dies kann sowohl als Einzelvereinbarung geschehen als auch im Rahmen einer grundsätzlichen Vereinbarung („Rahmenvertrag“ zur Auftragsverarbeitung) begleitet von konkretisierenden Einzel-Verträgen, welche die auftragsspezifischen Vertragsinhalte darstellen, als auch durch einen umfassenden Gesamtvertrag, in dem alle Regelungen enthalten sind. Ob sinnvollerweise ein Rahmenvertrag mit ergänzenden Einzelverträgen oder ein einzelner Gesamtvertrag abgeschlossen wird, kann nur im jeweiligen Einzelfall entschieden werden.

Das vorliegende Werk befasst sich grundsätzlich nur mit den speziellen Anforderungen an den AV-Vertrag, allgemeine Regelungen bleiben hierbei im Wesentlichen unberücksichtigt.

Lässt ein Verantwortlicher mehrere Verarbeitungen von ein und demselben Auftragsverarbeiter durchführen, so empfiehlt sich die Ausgestaltung des Vertrages in einem Auftragsverarbeitungs-Rahmenvertrag und ergänzenden Einzelverträgen, welche die jeweiligen auftragsspezifischen Details ergänzen.

Im Rahmenvertrag werden die allen Verarbeitungen zugrundeliegenden Vertragsinhalte geregelt. Hierzu können beispielsweise gehören:

- Umgang mit den Betroffenenrechten,
- die Rechte und Pflichten des Auftraggebers,
- der Umfang der Weisungsbefugnisse, die der Auftraggeber gegenüber dem Auftragnehmer hat,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- die bestehenden Pflichten des Auftragnehmers (Art. 28 DS-GVO),
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- Umgang mit Verstößen.

Evtl. können im Rahmenvertrag auch die Art der Daten wie auch die Kategorien betroffener Personen geregelt werden, sofern es sich in sämtlichen zu regelnden Verarbeitungsvorgängen um dieselben handelt.

Die Einzelverträge beinhalten die für die jeweilige spezifische Verarbeitung zu regelnden Vertragsinhalte. Typischerweise gehören hierzu

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten,

- zu treffende Schutzmaßnahmen.

2.2 Inhaltliche Anforderungen an einen AV-Vertrag

Unter Beachtung von Art. 28 DS-GVO und ErwGr. 81 ergeben sich die in den folgenden Abschnitten dargestellten Anforderungen, die im AV-Vertrag mindestens geregelt werden müssen.

Zu regelnde Vertragsbestandteile

1) Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3 S. 1 DS-GVO)
2) Umfang, Art und Zweck (Art. 28 Abs. 3 S. 1 DS-GVO) der vorgesehenen Verarbeitung von Daten
3) Die Art der Daten (Art. 28 Abs. 3 S. 1 DS-GVO)
4) Die Kategorien betroffener Personen (Art. 28 Abs. 3 S. 1 DS-GVO)
5) Die Gewährleistung der Betroffenenrechte (Art. 28 Abs. 3 S. 2 lit. e DS-GVO)
6) Rechte und Pflichten des Auftraggebers (Art. 28 Abs. 3 S. 1 DS-GVO)
7) Der Umfang der Weisungsbefugnisse, die der Auftraggeber gegenüber dem Auftragnehmer hat (Art. 28 Abs. 3 S. 1 sowie Art. 29 DS-GVO).
8) Die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers (Art. 28 Abs. 3 S. 2 lit. h DS-GVO)
9) Die bestehenden Pflichten des Auftragnehmers (Art. 28 DS-GVO)
10) Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen (Art. 28 Abs. 2, Art. 28. Abs. 3 S. 2 lit. d DS-GVO)
11) Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder gegen die im Auftrag getroffenen Festlegungen (Art. 28 Abs. 3 S. 2 lit. f sowie Art. 33 Abs. 2 DS-GVO)
12) Die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags (Art. 28 Abs. 3 S. 2 lit g DS-GVO)

3 Abgrenzung der Thematik

Diese Ausarbeitung befasst sich ausschließlich mit den datenschutzrechtlichen Anforderungen. Nicht Bestandteil dieser Ausarbeitung sind andere Anforderungen an Vorhaben, welche eine externe Verarbeitung beinhalten, seien sie rechtlicher Natur (wie z. B. Wirtschaftlichkeitsnachweise bzgl. einer Auftragsverarbeitung, wie sie in einigen Landesgesetzen gefordert werden oder auch Vertragsstrafen) oder Empfehlungen der entsprechenden Fachorgane (wie beispielsweise einer Freigabe durch die entsprechende Ethikkommission bei Forschungsvorhaben). Hier wird auf die gängige Literatur verwiesen.

4 Spezielle Fragestellungen

4.1 Wartung / Fernwartung

Auch wenn Art. 28 DS-GVO im Gegensatz zu § 11 BDSG die Wartung/Fernwartung nicht per Gesetz als eine Auftragsverarbeitung qualifiziert, sind diese Tätigkeiten weiterhin im Rahmen einer Auftragsverarbeitung abbildbar, da die bekannten Gründe, warum eine Wartung/Fernwartung einer Auftragsverarbeitung zuzurechnen ist, bestehen bleiben[3]. Insbesondere gilt, dass im Rahmen einer Wartung/Fernwartung der Dienstleister nicht über Mittel und Zwecke der Verarbeitung von personenbezogenen Daten entscheiden darf und der Dienstleister somit kein Verantwortlicher im Sinne der DS-GVO ist, sondern ein Auftragsverarbeiter.

4.2 Sozialdatenschutz

Die Regelungen bzgl. der Anforderungen an einen Vertrag zur Auftragsverarbeitung in § 80 SGB X werden durch die entsprechenden Regelungen in Art. 28 DS-GVO ersetzt. Der deutsche Gesetzgeber darf aufgrund fehlender Öffnungsklauseln bzgl. der Auftragsverarbeitung keine abweichenden Regelungen erlassen.

Das zuständige Bundesministerium für Arbeit und Soziales signalisierte bereits, dass das SGB X inkl. § 80 SGB X angepasst wird, jedoch kann noch nicht abgeschätzt werden, wann die Änderungen verabschiedet werden.

In der Übergangszeit kann es zu der oben geschilderten Problematik kommen, dass ein Gesetz grundsätzlich Geltung hat, bis es aufgehoben wird. Ändert der Gesetzgeber daher die Gesetze nicht, hat der Gesetzesanwender die Schwierigkeit, dass er einerseits das vorrangig geltende europäische Recht[5] beachten muss, andererseits die deutschen, eigentlich von den europäischen Vorgaben „überschriebenen“ Regelungen noch gelten.

4.3 Forschung

Auch im Rahmen von Forschungsvorhaben gelten bzgl. einer Auftragsverarbeitung die aus Art. 28 DS-GVO resultierenden Anforderungen. Erfolgt eine Verarbeitung personenbezogener oder personenbeziehbarer Daten[6] im Auftrag, muss ein den Anforderungen der DS-GVO genügender AV-Vertrag abgeschlossen werden.

[5] siehe z.B.

- Der Vorrang des EU-Rechts. [Online, zitiert am 2017-03-11]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3Al14548
- Amtsblatt der Europäischen Union, C 115, 09. Mai 2008, 17. Erklärung zum Vorrang: „[...]die Verträge und das von der Union auf der Grundlage der Verträge gesetzte Recht im Einklang mit der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union unter den in dieser Rechtsprechung festgelegten Bedingungen Vorrang vor dem Recht der Mitgliedstaaten haben“. . [Online, zitiert am 2017-03-11]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=OJ:C:2008:115:TOC

[6] Die DS-GVO definiert in Art. 4 Begrifflichkeiten, die z.T. mit den in Deutschland bekannten Begriffsdefinitionen übereinstimmen, z.T. aber auch abweichen.

4.4 Anonymisierung

Der Verordnungsgeber definiert unter Art. 4 DS-GVO zahlreiche Begriffe, trifft jedoch für die „Anonymisierung“ an keiner Stelle eine Aussage. Der Aufhebung des Personenbezugs könnte man sich wie folgt nähern:

Entsprechend dem Verständnis der Artikel-29-Datenschutzgruppe 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“[7]. Dabei ist ein Anonymisierungsverfahren „als eine Form der Weiterverarbeitung“ personenbezogener Daten mit dem Ziel ihrer Anonymisierung anzusehen[7]. Insofern 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“[8]. Dementsprechend ist eine Anonymisierung nur erlaubt, wenn ein Erlaubnistatbestand gemäß Art. 6 DS-GVO bzw. im Fall von besonderen Arten von Daten ein Erlaubnistatbestand nach Art. 9 DS-GVO vorliegt.

4.5 Schweigepflicht vs. Datenschutz

Vom Grundsatz her ist bei jeglichen Datenverarbeitungsvorgängen zwischen der rein datenschutzrechtlichen Ebene auf der einen sowie dem strafrechtlichen Berufsgeheimnisschutz (bzw. der Schweigepflicht) auf der anderen Seite zu differenzieren. Während die datenschutzrechtliche Ebene sich an die Institution, beispielsweise einen Krankenhausträger, richtet, betrifft der Berufsgeheimnisschutz den einzelnen Schweigepflichtigen, der mit den personenbezogenen Daten arbeitet.
Hinsichtlich der Frage des Verhältnisses zwischen dem Datenschutz auf der einen und der Schweigepflicht auf der anderen Seite existieren zwei Ansichten: In der einen Denkweise wird eine datenschutzrechtliche Verarbeitungserlaubnis für Patientendaten als strafrechtliche Offenbarungsbefugnis angesehen; diese Ansicht vertritt z. B. die Deutsche Krankenhausgesellschaft. Nach anderer Auffassung ist eine strafrechtliche Offenbarungsbefugnis durch datenschutzrechtliche Regelungen nicht möglich. Da nicht geklärt ist, welche der nachfolgend dargestellten Rechtsauffassungen die Zutreffende ist, muss jeder für sich selbst eine Entscheidung treffen, was als die zutreffende Rechtsauffassung anzusehen ist.

4.5.1 Auftragsverarbeitung als strafrechtliche Offenbarungsbefugnis

Eine Legitimation des Krankenhausträgers (also der Institution Krankenhaus), Daten im Rahmen einer Auftragsverarbeitung an einen Dritten offenbaren zu dürfen, jedoch den einzelnen Arzt bzw. die berufsmäßig tätigen Gehilfen unter Strafe zu stellen, ist nur schwer nachzuvollziehen, zumal von einem gleichen Schutzniveau auszugehen ist.

[7] 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
[8] Article 29 Data Protection Working Party. (2013) Opinion 03/2013 on purpose limitation. [Online, zitiert am 2017-02-25]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Aus diesem Grunde kann davon ausgegangen werden, dass das Gebot der Schweigepflicht gewahrt wird, sofern ein Datenschutzgesetz die Verarbeitung von Patientendaten ausdrücklich zulässt.
Ein Hinweis darauf ist, dass keine Rechtsprechung existiert, die die Frage klärt, ob bei Vorliegen einer datenschutzrechtlichen Verarbeitungserlaubnis dennoch eine Verletzung der ärztlichen Schweigepflicht vorliegen könnte. Das teilweise zitierte Urteil des Landgerichts Flensburg vom 05.07.2013 (Az.: 4 O 54/11) kann nicht als einschlägig angesehen werden. Gegenstand des Rechtsstreits war die ehrenamtliche Beauftragung eines externen Dritten mit der Wartung der EDV- sowie Telefon-Anlage einer Arztpraxis. Hierfür lagen weder eine gesetzliche Grundlage, noch entsprechende Einwilligungserklärungen der Patienten, noch ein Vertrag über eine Auftragsdatenverarbeitung vor. Das Gericht kam konsequenterweise zu dem Schluss, dass dadurch gegen die ärztliche Schweigepflicht verstoßen worden ist. Daneben existiert noch eine ältere Entscheidung des Oberlandesgerichts Düsseldorf aus 1996 (Urteil vom 20.08.1996, Az.: 20 U 139/95). Auch diese Entscheidung trägt nicht die Auffassung, dass eine Strafbarkeit anzunehmen ist.
Im Ergebnis kann also davon ausgegangen werden, dass auch das Gebot der Schweigepflicht gewahrt ist, sofern ein Gesetz – mit gleichem Schutzniveau – die Verarbeitung von Patientendaten ausdrücklich zulässt. Für die Zukunft wird diese Auffassung dadurch gestärkt, dass die Regelung, auf die sich die gegenteilige Ansicht bislang beruft (§ 1 Abs. 3 S. 2 BDSG), voraussichtlich infolge des durch die DS-GVO bedingten gesetzlichen Anpassungsbedarfs gestrichen wird.
Sofern Aufsichtsbehörden diesbezüglich eine gegenteilige Auffassung vertreten, kann die hier dargestellte Argumentation der Deutschen Krankenhausgesellschaft dem entgegen gehalten werden.

4.5.2 Auftragsverarbeitung stellt keine strafrechtliche Offenbarungsbefugnis dar

§ 1 Abs. 3 S. 2 BDSG gewährleistet, dass der auf spezifische Berufsgruppen bezogene Sonderschutz, wie in § 203 StGB dargestellt, nicht durch das BDSG verringert wird[9]. § 1 Abs. 3 S. 2 BDSG stellt eindeutig klar, dass das BDSG in keiner Weise in den Schutzbereich dieser Normen, die einen besonderen Schutzbereich bzgl. der besonderen Berufs- oder Amtsgeheimnisse darstellen, eingreift. Dementsprechend kann § 11 BDSG keine Offenbarungsbefugnis im Sinne von § 203 StGB darstellen. Diese Rechtsmeinung wird von einer großen Anzahl von Autoren vertreten[10].

[9] Dix A. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Rn 175ff zu §1
[10] Siehe z.B.:

- Buchner B. (2013) Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht. MedR: 337 - 342
- 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
- Giesen T. (2012) Zum Begriff des Offenbarens nach § 203 StGB im Falle der Einschaltung privatärztlicher Verrechnungsstellen. NStZ: 122ff
- Jandt S, Roßnagel A, Wilke D. (2011) Outsourcing der Verarbeitung von Patientendaten - Fragen des Daten- und Geheimnisschutzes. NZS: 641ff
- Klein H. (2010) Schweigepflicht versus Offenbarungspflicht. RDG: 172ff
- Kroschwald S, Wicker M. (2012) Kanzleien und Praxen in der Cloud – Strafbarkeit nach §203 StGB. CR: 758ff
- Leisner W. (2010) Einschaltung Privater bei der Leistungsabrechnung in der Gesetzlichen Krankenversicherung - Verfassungsrechtliche Vorgaben für eine anstehende gesetzliche Neuregelung. NZS: 129ff

Auch die Kassenärztliche Vereinigung Bayerns beurteilt datenschutzrechtliche Regelungen und insbesondere eine Auftragsverarbeitung als gegenüber der aus § 203 StGB resultierenden Schweigepflicht als nachrangiges Recht.[11]

Wenngleich es keine den Autoren bekannten Urteile aus dem Strafrecht gibt, die das Verhältnis zwischen datenschutzrechtlicher Verarbeitungserlaubnis und strafrechtlicher Offenbarungsbefugnis klären, wurde § 203 StGB schon mehrfach in zivilen Prozessen thematisiert. Hierbei wurde festgestellt, dass die aus § 203 StGB resultierende Schweigepflicht gegenüber Datenschutzbestimmungen als vorrangiges Recht anzusehen ist und damit verbunden, dass insbesondere bei einer datenschutzrechtlichen Auftragsdatenverarbeitung von Patientendaten immer zugleich auch eine Datenoffenbarung i.S.v. § 203 Abs. 1 StGB vorliegt[12].

Mehrere Landeskrankenhausgesetze bzw. bereichsspezifische Landesgesetze geben zudem als Voraussetzung für eine zulässige Auftragsverarbeitung vor, dass beim Auftragnehmer eine den Voraussetzungen des § 203 StGB entsprechende Schweigepflicht sichergestellt sein muss, so beispielsweise

- Baden-Württemberg (§ 48 Landeskrankenhausgesetz BW)
- Berlin (§ 24 Abs. 1 Landeskrankenhausgesetz Berlin)
- Nordrhein-Westfallen (§ 7 Abs. 3 Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen)
- Rheinland-Pfalz (§ 36 Abs. 9 Landeskrankenhausgesetz RP)
- Sachsen (§ 33 Abs. 10 Sächsisches Krankenhausgesetz)
- Thüringen (§ 27b Thüringer Krankenhausgesetz)

Desgleichen finden sich entsprechende Regelungen auch in Gesetzen der Kirche, z. B. in § 6 „Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern“ in der Diözese Hildesheim oder der entsprechenden Regelung im Bistum Osnabrück oder dem Erzbistum Hamburg.

Das Verhältnis zwischen datenschutzrechtlicher Verarbeitungserlaubnis und strafrechtlicher Offenbarungsbefugnis wird dadurch jedoch nicht geklärt, da die zitierten Gesetze zur Frage, ob bei Einhaltung sämtlicher in einem Landeskrankenhausgesetz oder bereichsspezifischen Landesgesetz vorgeschriebenen Voraussetzungen für eine Auftragsverarbeitung dennoch eine Verletzung der ärztlichen Schweigepflicht vorliegen könnte, einerseits keine Aussage enthalten, andererseits aber auch keine Erlaubnisnorm im Sinne des Strafrechts enthalten. Daher kann die Auffassung vertreten werden, dass eine datenschutzrechtliche Auftragsverarbeitung keine Offenbarungsbefugnis im Sinne des § 203 StGB darstellt.

- Lewinski K. (2004) Schweigepflicht von Arzt und Apotheker, Datenschutzrecht und aufsichtsrechtliche Kontrolle. MedR: 95ff
- Menzel HJ. (2013) Auftragsdatenverarbeitung im Sozial- und Gesundheitswesen. RDV: 59ff
- Oetterich D (2013) Auslagerung von Dienstleistungen im Widerspruch zum Berufsrecht? DStR: 2482ff
- Szalai S, Kopf R. (2012) Verrat von Mandantengeheimnissen - Ist Outsourcing strafbar nach §203 StGB? ZD: 462ff

[11] Kassenärztliche Vereinigung Bayerns (2016) Datenschutz in der Arzt-/Psychotherapeutenpraxis. Kap. 6.2 „Datenverarbeitung durch externe Dritte“. [Online, zitiert am 2017-01-27]; Verfügbar unter https://www.kvb.de/fileadmin/kvb/dokumente/Praxis/Infomaterial/Praxisbetrieb/KVB-Broschuere-Datenschutz-in-der-Praxis.pdf

[12] So z. B.

- OLG Düsseldorf, Urteil vom 20.08.1996, AZ 20 U 139/95
- KG, Urteil vom 20.08.2010, AZ 1 Ws (B) 51/07 - 2 Ss 23/07 (317 OWi 3235/05)
- LG Flensburg, Urteil vom 05.07.2013, AZ- 4 O 54/11

4.5.3 Aussicht

Um dieser dargestellten Rechtsunsicherheit zu begegnen, sind derzeit gesetzliche Anpassungen in § 203 StGB geplant[13]. Desgleichen ist eine Anpassung des Zeugnisverweigerungsrechts (§ 53a StPO) vorgesehen[14]. In beiden Fällen würden auch externe Personen, welche den Berufsgeheimnisträger in seiner Arbeit unterstützen, zu den Adressaten der jeweiligen Norm zählen. Die diesbezüglichen Entwicklungen bleiben abzuwarten.

[13] Vgl. Regierungsentwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 15.12.2016. [Online, zitiert am 2017-02-25] Verfügbar unter http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.html

[14] BT-Drucksache 18/9521: Gesetzentwurf zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Berufe vom 05.09.2016. . [Online, zitiert am 2017-02-25] Verfügbar unter http://dipbt.bundestag.de/extrakt/ba/WP18/762/76268.html

5 Vorbedingungen für einen AV-Auftrag

5.1 Auswahl des Auftragsverarbeiters/Auftragnehmers

Generell gilt, dass nur Auftragnehmer beauftragt werden dürfen, die hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen getroffen werden, welche den Anforderungen der DS-GVO genügen und den Schutz der Daten und der Rechte betroffener Personen gewährleisten. Ferner sind auch Aspekte wie „Fachwissen“, „Zuverlässigkeit“ sowie „Ressourcen“ des Auftragsverarbeiters mit zu berücksichtigen. Diese Anforderungen ergeben sich, unabhängig davon, dass sie in der Verordnung (Art. 28 Abs. 1 sowie ErwGr. 81 DS-GVO) stehen, bereits aus der Tatsache, dass es sich bei Gesundheitsdaten um „besondere Kategorien personenbezogener Daten“ handelt, für die ein entsprechend hoher Schutzbedarf gilt.

Eine Auswahl kann im Ergebnis nur als „geeignet“ getroffen angesehen werden, sofern sie mit dem Zweck erfolgt ist, einen Dienstleister mit einem angemessenen Datenschutzniveau auszuwählen[15]. Dies gilt auch dann, wenn nur ein einziger Anbieter zur Verfügung steht.

5.2 Erlaubnistatbestände zur Auftragsverarbeitung (Landesebene)[16]

In einigen Gesetzen werden Anforderungen gestellt, an deren Erfüllung die Vergabe eines Auftrags an eine Stelle außerhalb der Einrichtung geknüpft ist. D. h., die Verarbeitung von Patientendaten im Auftrag ist z. B. 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 informiert wurde oder
d) die für den Auftraggeber zuständige Aufsichtsbehörde vor Auftragsvergabe um Erlaubnis gebeten wurde.

Diese Regelungen beinhalten keine Anforderungen an die Vertragsgestaltung selbst, sondern stellen vielmehr zusätzliche Bedingungen im Sinne von Art. 9 Abs. 4 DS-GVO dar. D. h. diese Regelungen würden auch nach dem 25. Mai 2018 gelten, sofern die Landesgesetzgeber hier keine Änderung vornehmen. Die Entwicklungen bleiben hier abzuwarten.

Allerdings spricht Einiges dafür, dass Art. 9 DS-GVO für die *Art* der Daten, nicht für den Ort, an dem die Daten verarbeitet werden, gilt. Regelungen, wie beispielsweise

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

[16] Auch das jeweilige Landesrecht (Landesdatenschutzgesetze, datenschutzrechtliche Bestimmungen in Landeskrankenhausgesetzen usw.) muss entsprechend den Vorgaben der EU DS-GVO überarbeitet werden. D. h. hier werden sich Änderungen ergeben. Daher muss hier die diesbezügliche Entwicklung genau betrachtet werden. Gleiches gilt für Bundesgesetze, wie z. B. dem Sozialdatenschutz in SGB X.

in Baden-Württemberg[17] wären somit unwirksam. Hier eine Auflistung, in welchem Bundesland welche Anforderungen gelten:

	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. §12 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 öffentlichen Krankenhäuser Berlins, jedoch gelten für andere Gesundheitseinrichtungen die Vorgaben des Landesdatenschutzgesetzes nur für öffentliche Auftraggeber

	Niedersachsen (§6 NDSG)	Nordrhein-Westfalen (§ 7 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

[17] § 48 Landeskrankenhausgesetz Baden-Württemberg beschränkt in Abs. 1 die Datenverarbeitung auf ein Krankenhaus, in Abs. 2 auf „automatisierte Verarbeitung in Rechenzentren“; beides sind als unzulässige Einschränkungen der Regelungen der DS-GVO anzusehen und nach Wirkeintritt der DS-GVO wahrscheinlich als ungültig anzusehen

5.3 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 (siehe hierzu auch Kapitel 4.2). § 80 Abs. 5 SGB X lautet: „*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 Anzeige[18] gegenüber der für den Auftraggeber zuständigen Aufsichtsbehörde – 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.

5.4 Literatur

1) Eckhardt J, Kramer R. (2016) Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools. DuD: 144-149
2) Härting N. (2016) Auftragsverarbeitung nach der DSGVO. ITRB: 137-140
3) Müthlein T. (2016) ADV 5.0 - Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 74-87
4) Schmitz B, von Dall’Armi J. (2016) Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? Wie Daten künftig von Dienstleistern verarbeitet werden müssen. ZD: 427-432

[18] Eine solche Anzeige beinhaltet i.d.R. auch eine entsprechende Prüfung durch die Aufsichtsbehörde

6 Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union (ebenfalls gebräuchlich: AEU-Vertrag)
AV	Auftragsverarbeitung
Alt.	Alternative
Art.	Artikel
Artt.	Artikel (Mehrzahl)
BayKHG	Bayerisches Krankenhausgesetz
BbgDSG	Brandenburgisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BO	Berufsordnung
BremKHDSG	Bremisches Krankenhausdatenschutzgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
bvitg	Bundesverband Gesundheits-IT e.V.
DKG	Deutsche Krankenhausgesellschaft e.V.
DS-GVO	Datenschutz-Grundverordnung
DSG-LSA	Datenschutzgesetz Sachsen-Anhalt
EG	Europäische Gemeinschaft
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
GDSG	Gesundheitsdatenschutzgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
HDSG	Hessisches Datenschutzgesetz
HKHG	Hessisches Krankenhausgesetz
HmbKHG	Hamburgisches Krankenhausgesetz
lit	littera (= Buchstabe).
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	Gesetz gegen den unlauteren Wettbewerb

Kommentierter Muster-AV-Vertrag

Auftragsverarbeitungsvertrag zwischen

Name
Anschrift, vertreten durch
(Verantwortlicher im Sinne der DS-GVO, nachfolgend „Auftraggeber“ genannt)

und

Name
Anschrift, vertreten durch
(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „Auftragnehmer“ genannt)

Präambel[19]

Alt. 1: Existierender Hauptvertrag

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag

……

(im Folgenden Hauptvertrag genannt) beschriebenen Auftragsverarbeitung ergeben.

Sämtliche in diesem Vertrag 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 bzw. kommen können.

Hinweis:
Gegenstand dieses Vertrages sind ausschließlich datenschutzrechtliche Regelungen zur Auftragsverarbeitung. Strafrechtliche Bestimmungen wie beispielsweise § 203 StGB können nicht Vertragsgegenstand sein.

Alt. 2: Hauptvertrag liegt nicht vor

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den in § 2 Gegenstand des Auftrags“ dargestellten Leistungen ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit der Auftragserfüllung 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 bzw. kommen können.

[19] Präambel ist je nach Vertragsart ggfs. anzupassen, siehe Kapitel 2 „Einordnung des AV-Vertrages in Gesamtregelwerke“ auf Seite 12

Hinweis:
Gegenstand dieses Vertrages sind ausschließlich datenschutzrechtliche Regelungen zur Auftragsverarbeitung. Strafrechtliche Bestimmungen wie beispielsweise § 203 StGB können nicht Vertragsgegenstand sein.

Kommentierung Präambel

Gegenstand dieses Vertragsmusters ist in Alternative 1 die Konstellation, dass neben einem bereits existierenden gesonderten, die eigentliche Leistung beschreibenden Hauptvertrag nunmehr in dem AV-Vertrag nur die datenschutzrechtlichen Anforderungen an die in dem Hauptvertrag beschriebene AV geregelt werden. Insofern stellt der AV-Vertrag lediglich eine datenschutzrechtliche Konkretisierung dar.

In der dafür vorgesehenen Zeile ist der Name des Hauptvertrages nebst Datum genau zu benennen.

§ 203 StGB und Auftragsverarbeitung

Die Verantwortung für die Wahrung der ärztlichen Schweigepflicht obliegt ausschließlich dem Auftraggeber; diese Verantwortung kann nach heutiger Rechtslage vom Auftraggeber nicht vertraglich an einen Auftragnehmer delegiert werden. Strafrechtliche Regelungen können daher nicht Gegenstand dieses Mustervertrages sein. Bzgl. des Verhältnisses der datenschutzrechtlichen Befugnis zur Auftragsverarbeitung und dem strafrechtlichen Tatbestand des unbefugten Offenbarens siehe Kapitel 4.5 auf Seite 15.

Um die Wahrung des einem Berufsgeheimnisträger anvertrauten Geheimnisses so gut wie möglich abzusichern werden folgende Möglichkeiten empfohlen:

- eine formelle Verpflichtung nach dem Verpflichtungsgesetz
- eine Verpflichtung nach §17 UWG. (siehe entsprechenden Abschnitt in der Kommentierung § 7, Abschnitt „Verpflichtung des vom Auftragnehmer eingesetzten Personals“ auf Seite 55).

Im Gegensatz zu einer datenschutzrechtlichen Verpflichtung entsprechend Art. 28 DS-GVO (siehe Beispiel für Verpflichtungserklärung auf Seite 94) wird durch eine Verpflichtung der obigen Alternativen ein Straftatbestand bei einer unerlaubten Datenweitergabe durch den Auftragnehmer begründet.

Formelle Verpflichtung der Auftragsverarbeitenden

Eine formelle Verpflichtung nach Verpflichtungsgesetz kann nur eine öffentliche Stelle durchführen, d. h. diese Möglichkeit ist ausschließlich öffentlichen Stellen vorbehalten. In der Regel wird der Auftragnehmer gegenüber dem von ihm eingesetzten Personal keine formelle Verpflichtung vornehmen können, da er dazu eine öffentliche Stelle sein müsste.

Die Bundesländer haben in ihren jeweiligen Verordnungen beschrieben, wer eine entsprechende Verpflichtung vollziehen kann.

Wenn möglich, sollte eine datenschutzrechtliche Verpflichtung des vom Auftragnehmer eingesetzten Personals entsprechend dem Verpflichtungsgesetz durchgeführt werden, sei es vom Auftraggeber oder vom Auftragnehmer.

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
5) Martini M. (2016) Art. 28 DS-GVO, Rn. 43 „Verpflichtung zur Vertraulichkeit bzw. Verschwiegenheit“ in Paal/Paul (Hrsg.) Datenschutz-Grundverordnung. C.H.Beck Verlag. ISBN 978-3-406-69570-4

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 2 TMG sowie Landesdatenschutzgesetz/Landeskrankenhausgesetz [hier bitte das jeweils geltende Rechtswerk benennen]. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, Landesrecht, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung

Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(3) Verarbeitung im Auftrag

Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

(4) 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-AV-Vertrages wird in den Zeilen 2-6 daher auf die in DS-GVO, UWG und TMG enthaltenen Definitionen verwiesen, in den Zeilen 9 - 27 werden die dort nicht enthaltenen Begriffe „Anonymisierung“, „Unterauftragnehmer“, „Verarbeitung im Auftrag“ sowie „Weisung“ definiert.

Literatur

1) Artikel-29-Datenschutzgruppe. (2007) Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“. [Online, zitiert am 2017-02-23]; 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 2017-02-23]; 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 2017-02-23]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

§ 2 Gegenstand des Auftrags

Alt. 1

Gegenstand der Vereinbarung ist die Verarbeitung 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 Kategorien von Daten(arten), insbesondere
     - rassische oder ethnische Herkunft,
     - religiöse Überzeugung
     - weltanschauliche (philosophische) Überzeugung
     - politische Überzeugungen/Meinungen
     - Gesundheit (inkl. genetischer Daten)
     - Biometrischen Daten zur (eindeutigen) Identifizierung einer Person
     - Gewerkschaftszugehörigkeit
     - Sexualleben oder der sexuellen Orientierung

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

b. Der Zugriff auf die Daten bzw. die Datenerhebung erfolgt wie folgt:

   Alt. 1.1
   - Übermittlung durch den Auftraggeber über: ……

   Alt. 1.2
   - Beauftragung durch den Auftraggeber: ……

c. 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, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann: ……
   - Hardware-Diagnose per Fernzugriff für folgende Hardwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann: ……
   - Software-Prüfung/Wartung per Fernzugriff für folgend(e) Softwareprodukt(e), bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann: ……
   - ……

Alt. 2

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

- ☐ Personenstammdaten (z. B Mitarbeiter, Kooperationspartner, nicht med. Patientendaten)
- ☐ Medizinische Patientendaten (Befunde, Diagnosen, …)
- ☐ Kontaktdaten/Kommunikationsdaten (z. B. IP-Adressen, 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

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im … Vertrag der Parteien vom … (nachstehend „Hauptvertrag“ genannt“) und in der darin enthaltenen Leistungsbeschreibung konkretisiert sind. Im Einzelnen sind insbesondere folgende Daten Bestandteil der Datenverarbeitung:

Art der Daten	Zweck der Datenverarbeitung	Kreis der Betroffenen

Opt. § 2.1 Leistungen des Auftragnehmers

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

- … [Aufzählung der vom Auftragnehmer zu erbringenden Leistungen]

Kommentierung § 2

§ 2 besteht aus genau einem Absatz, zu dem jedoch 3 alternative Formulierungen angeboten werden. D. h. für einen konkreten Vertrag muss genau eine Alternative ausgewählt werden. Welche der drei Alternativen zu wählen ist, ist dabei nicht über die Aufgabe bestimmt, sondern spiegelt eher den Stil der Vereinbarung. Alternative 1 ist die längste und erläutert viele Aspekte an Hand von Aufzählungen, Alternative 2 erlaubt es, mit einer Ankreuzliste schnell aus einer Vorlage einen konkreten Vertrag zu formen, während Alternative 3 die genaue Beschreibung der einzelnen Zugriffsszenarien ermöglicht und damit die größte Flexibilität und Genauigkeit aber auch den größten Aufwand bietet.

Meistens wird der genaue Gegenstand des Auftrags in einem Hauptvertrag dargestellt sein, sodass an dieser Stelle auf den entsprechenden Vertrag verwiesen werden kann. Dies ist exemplarisch bei § 2 Alt. 1 und Alt. 3 dargestellt. Gleiches gilt für die Dauer der Beauftragung (§ 4).

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

Der Kreis der Betroffenen ist dabei so konkret wie möglich zu erfassen, pauschale Angaben wie „Kundendaten“ verbieten sich[20]. Dabei müssen der Zweck, der betroffene Personenkreis und der beabsichtigte Umgang der Daten einander zuordenbar angegeben werden[15]. 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 Alt. 3 dargestellt.

Konkretisierung des Auftrags

Meistens wird im eigentlichen Vertrag nicht auf die datenschutzrechtlichen Aspekte wie die Art der Unterstützung (z. B. Administration der Patientenverwaltung) oder die Nennung der betroffenen Personenkategorien (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 AV-Vertrags (§ 2 und in § 2.1) beschrieben werden.

Literatur

1) Hoeren T. (2010) Das neue BDSG und die Auftragsverarbeitung. DuD: 688-691
2) Müthlein T. (2016) ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 74-87

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

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

§ 3 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO).

Opt. (2) Die Inhalte dieses AV-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.

(3) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

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

Kommentierung § 3

Verpflichtung Art. 28 DS-GVO

Mit der Anpassung/Änderung des Bundesdatenschutzgesetzes entfällt auch die Verpflichtung auf das Datengeheimnis entsprechend § 5 BDSG. Die DS-GVO enthält dem BDSG ähnelnde Regelungen, aber keine identischen.

Ein § 5 S. 1 BDSG entsprechendes Verbot zur unbefugten Verarbeitung personenbezogener Daten ergibt sich aus Art. 6 Abs. 1 bzw. Art. 9 Abs. 1 DS-GVO, wodurch das Datengeheimnis nach wie vor begründet ist.

Eine vertragliche Verpflichtung, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden oder einer gesetzlichen Verschwiegenheitspflicht unterliegen, findet sich im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 lit. b DS-GVO. Dies gilt sowohl für die beim Auftraggeber als auch die beim Auftragnehmer eingesetzten Personen. Außerhalb der Auftragsverarbeitung kennt die DS-GVO jedoch keine entsprechende Verpflichtung.

Eine § 5 S. 3 BDSG entsprechende Regelung, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht, findet sich in dieser Form in der DS-GVO nicht.[21] Grundsätzlich ergibt sich ein Verbot der Weitergabe von während einer Tätigkeit erhaltener Informationen nach Beendigung der Tätigkeit aber bereits aus Art. 6 Abs. 1 bzw. Art. 9 Abs. 1 DS-GVO, da ein Erlaubnistatbestand zur Verarbeitung der Daten nur während der Tätigkeit besteht und eine Weitergabe von Daten nach Beendigung der Tätigkeit mangels Verarbeitungserlaubnis demnach verboten ist.

Im Rahmen der Auftragsverarbeitung sollten sich die Vertragspartner auf die Inhalte der Verpflichtungserklärung einigen. Grundsätzlich ist hierbei auch ein mögliches Mitbestimmungsrecht von Mitarbeitervertretungen zu beachten.

Da derzeit noch keine Musterformulare bzgl. einer Verpflichtung nach § 28 DS-GVO existieren, befindet sich in Anlage 3 auf Seite 94 ein Formulierungsvorschlag.

Literatur

(1) Eckhardt J, Kramer R. (2016) Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools. DuD: 144-149
(2) Härting N. (2016) Auftragsverarbeitung nach der DSGVO. ITRB: 137-140
(3) Holländer C. (2014) Auftragsdatenverarbeitung: Aus der Praxis der Aufsichtsbehörden. ITRB: 115-116
(4) Koós C, Englisch B. (2014) Eine "neue" Auftragsdatenverarbeitung? - Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs. ZD: 276-285
(5) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft

[21] Die derzeit auf Grundlage von § 5 BDSG verwendeten Verpflichtungserklärungen müssen daher gegebenenfalls angepasst werden, es sei denn der Gesetzgeber trifft im Zuge der notwendigen Gesetzesanpassungen eine vergleichbare Regelung. Die diesbezüglichen Entwicklungen bleiben abzuwarten.

(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

§ 4 Dauer des Auftrags

Alt. 1 zu Abs. 1

(1) Die Dauer des Auftrags ist in § … des Hauptvertrags zwischen Auftraggeber und Auftragnehmer geregelt, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

Alt. 2 zu Abs. 1

(1) Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

Alt. 3 zu Abs. 1

(1) Die Laufzeit dieses AV-Vertrages endet am …, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

Alt. 4 zu 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 AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

Kommentierung § 4

Gesetzlich vorgeschrieben ist, dass die Dauer und damit auch die Beendigung der AV-Dienstleistung vertraglich geregelt werden (Art. 28 Abs. 3 S.1 DS-GVO). Damit kann die Dauer des Auftrags befristet werden, jedoch kann der Auftrag auch unbefristet erteilt werden. In letzterem Fall müssen jedoch die Art und Weise der Beendigung des Vertrages – durch entsprechende Kündigungsregelungen – vereinbart werden.

In Alt. 3 zu Abs. 1 ist vorgesehen, dass die Laufzeit des AV-Vertrages zu einem bestimmten Zeitpunkt endet, sofern sich aus den Bestimmungen des AV-Vertrages nicht etwas anderes ergibt. Diese Regelung hat den Hintergrund, dass in einem AV-Vertrag regelmäßig auch Bestimmungen enthalten sein können, die Verpflichtungen beinhalten, welche eine Beendigung der Auftragsverarbeitung ggf. nicht erlauben. Z. B. ist „Löschen“ eine Form der Verarbeitung. Löscht ein Auftragnehmer Daten nach Beendigung des Vertrages, wird er bei wörtlicher Auslegung des Gesetzes zum Verantwortlichen (Art. 28 Abs. 10 DS-GVO) und darf die Löschung - aber auch die weiter fortdauernde Speicherung - nur mit einem Erlaubnistatbestand durchführen. Zudem gab der Auftragnehmer die personenbezogenen Daten in diesem Fall ggf. ohne Rechtsgrundlage an den Auftragnehmer (bzw. den „neuen“ Verantwortlichen) weiter und verstößt damit gegen das geltende Recht. Daher ist in Alt. 3 eine entsprechende Regelung enthalten, entsprechend welcher der AV-Vertrag ggf. verlängert wird, bis alle sich aus dem AV-Vertrag ergebenden Leistungen erbracht wurden.

Kündigungsbestimmungen sind in einem AV-Vertrag für den Fall überflüssig, dass der Hauptvertrag auch für den AV-Vertrag bereits entsprechende Regelungen enthält.

Literatur

1) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
2) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
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

§ 5 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. 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.

Alt. 1 zu Abs. 2:

(2) Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

Alt. 2 zu Abs. 2:

(2) Die Weisungen des Auftraggebers werden vom Auftraggeber dokumentiert und dem Auftragnehmer unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

Alt. 1 zu Opt. Abs. 3:

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer vom Auftragnehmer als wesentlich angesehenen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

Alt. 2 zu Opt. Abs. 3:

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

Alt. 3 zu Opt. Abs. 3:

(3) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem

Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

(4) 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. (5) 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

Kommentierung § 5

Die gesetzlichen Vorschriften schreiben dem Auftraggeber vor, dass in einem AV-Vertrag der Umgang mit den Daten durch den Auftragnehmer beschrieben werden muss. Insbesondere ist in der DS-GVO vorgeschrieben, dass der Auftragnehmer nur auf Weisung des Auftraggebers tätig werden darf und dies im Vertrag festgehalten werden muss (§ 5). Es sollte daher vertraglich geregelt werden, wer diese Dokumentation vornimmt. Zugleich sollte der nicht-dokumentierende Vertragspartner immer eine Kopie der Dokumentation erhalten, damit er die Richtigkeit der Dokumentation zeitnah überprüfen kann.

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 von Patienten abzuwenden, so muss der Auftraggeber unverzüglich eine schriftliche Beauftragung nachreichen. Ohne entsprechende Weisung ist der Auftragnehmer nicht befugt, Daten in anderer Form zu verarbeiten. Daher ist es aus Sicht des Auftragnehmers wichtig, dass jede Weisung schriftlich erfolgt und er so den Nachweis des Tätigwerdens auf Weisung des Auftraggebers auch gegenüber der Aufsichtsbehörde erbringen kann.

Nachträgliche Änderung der vertraglich vereinbarten Leistungen durch den Auftraggeber

Gemäß § 5 Abs. 3 sind nach Vertragsabschluss erfolgende Änderungen des vertraglich vereinbarten Verarbeitungsgegenstandes und Verfahrensänderungen von der Weisungsbefugnis des Auftraggebers gedeckt („einseitige Möglichkeit der Änderung der vertraglichen vereinbarten Leistungen") und entsprechend zu dokumentieren. Dies ist erforderlich, wenn z. B. auf Änderungen der gesetzlichen Regelungen bzgl. der Verarbeitung der Daten reagiert werden soll, ohne dass eine Neuverhandlung des Vertrages notwendig ist.

Für die Rechtsfolgen einer wesentlichen Änderung des Auftrags durch den Auftraggeber sind sodann drei unterschiedliche Regelungsalternativen vorgesehen, von denen je nach Vertragsausgestaltung eine Variante auszuwählen ist. Nach Alternative 1 steht dem Auftragnehmer bereits dann ein außerordentliches Kündigungsrecht zu, wenn er die Änderung persönlich als wesentlich einstuft[22]. Demgegenüber ist in den Alternativen 2 und 3 die wesentliche Änderung des Auftrags Voraussetzung für ein Kündigungsrecht des Auftragnehmers. Der Unterschied der Alternativen 2 und 3 besteht darin, dass der Auftragnehmer nach Alternative 2 bei Vorliegen einer wesentlichen Änderung ein außerordentliches Kündigungsrecht hat, während ihm nach Alternative 3 bei Vorliegen einer

[22] Dem EuGH-Urteil vom 19. Juni 2008 (AZ C-454/06, Rn 36,37 [Online, zitiert am 2017-01-27] Verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=69189&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1) folgend ist „wesentliche Änderung“ wie folgt auszulegen: Änderung des ursprünglichen Auftrags sind als wesentlich anzusehen, wenn sie den Auftrag in großem Umfang auf ursprünglich nicht vorgesehene Dienstleistungen erweitern oder das wirtschaftliche Gleichgewicht des Vertrags in einer im ursprünglichen Auftrag nicht vorgesehenen Weise verändern

wesentlichen Änderung ein ordentliches Kündigungsrecht zusteht. Der Auftragnehmer hat bei allen Alternativen zunächst ein Widerspruchsrecht und kann erst dann kündigen, wenn der Auftraggeber trotz des Widerspruchs des Auftragsnehmers auf der Änderung des Auftrags besteht. Bei der Auswahl einer Regelungsalternative ist zu berücksichtigen, dass die Möglichkeit einer außerordentlichen Kündigung durch den Auftragnehmer im Falle einer wesentlichen Änderung des Auftrags zu einer sofortigen Beendigung des von der Weisung betroffenen AV-Vertrages führen kann. Bei einer ordentlichen Kündigung läuft das Vertragsverhältnis bis zum Eintritt der Kündigung (Kündigungsfristen regeln!) unverändert weiter und der Auftragnehmer muss die vertraglich vereinbarte Leistung erbringen.

Literatur

(1) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
(2) Eckhardt J, Kramer R. (2016) Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools. DuD: 144-149
(3) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
(4) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
(5) 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 Leistungsort[23]

Alt. 1 zu Abs. 1:

(1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in Anhang 1 vereinbarten Leistungsstandorten in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

Alt. 2 zu Abs. 1:

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in Anhang 1 vereinbarten Leistungsstandorten der Unterauftragnehmer in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

Alt. 3 zu Abs. 1:

(1) Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland. Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.

Alt. 4 zu Abs. 1:

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in Anhang I dargestellt. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.

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

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über

[23] Für den Fall der Notwendigkeit eines spezifischen Leistungsorts (etwaige Vorgaben aus anderen rechtlichen Regelungen) ist dieses vertraglich verbindlich zu regeln.

Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

Opt (6) Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DS-GVO wird durch den Auftragnehmer gewährleistet.

(7) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend 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.

(8) 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 § 6

Im Gegensatz zum BDSG erlaubt die DS-GVO eine Auftragsverarbeitung überall auf der Welt. Es geht ausschließlich darum, dass das von der DS-GVO definierte Schutzniveau am Ort der Verarbeitung gewährleistet wird.

Verarbeitung innerhalb der EU

Der freie Verkehr personenbezogener Daten, zu denen auch die vom Landesrecht adressierten Patientendaten gehören, darf aus Gründen des Schutzes betroffener Personen bei der Verarbeitung ihrer Daten weder eingeschränkt noch verboten werden (Art. 1 Abs. 3 DS-GVO[24]). Somit dürfen auch datenschutzrechtliche Bestimmungen keine Grundlage für innereuropäische Verkehrsbeschränkungen sein[25].

Unter dem Aspekt, dass die DS-GVO das Datenschutzniveau innerhalb ihres Geltungsbereichs auf ein einheitlich hohes Niveau hebt, ist diese Regelung auch nachvollziehbar. ErwGr. 6 der DS-GVO stellt fest, dass „private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen“ und „auch natürliche Personen Informationen öffentlich weltweit zugänglich“ machen. Diese Entwicklungen „erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union“ (ErwGr. 7). Wird dieser Rechtsrahmen innerhalb der EU jedoch gewährleistet, ist eine Beschränkung der (legitimen) Verarbeitung personenbezogener Daten auf bestimmte Örtlichkeiten aus Gründen des Datenschutzes nicht notwendig; alle weisen ja dasselbe Datenschutzniveau, zumindest aber ein vergleichbares auf. Entsprechend führt ErwGr. 13 aus, dass „der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten“ werden darf.

Unter Berücksichtigung von Art. 26 Abs. 2 AEUV[26] ist auch offensichtlich, dass aus Sicht des europäischen Gedankens eine (unnötige) Beschränkung innerhalb der europäischen Binnengrenzen nicht mit dem Vertrag über die Arbeitsweise der Europäischen Union vereinbar ist: der „freie Verkehr von Waren, Personen, Dienstleistungen und Kapital“ muss gewährleistet sein.

Auftragsverarbeitung außerhalb der EU / 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 Auftragsverarbeitung mit einem deutschen Standardvertrag alleine nicht zulässig ist.

[24] EUR-Lex: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [Online, zitiert am 2017-01-02] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1483339883994&uri=CELEX:32016R0679

[25] Paal B, Pauly D. (2017) Datenschutz-Grundverordnung: DS-GVO. Art. 1 Rn. 13 C.H.Beck Verlag, 1. Auflage. ISBN 978-3-406-69570-4

[26] Vertrag über die Arbeitsweise der Europäischen Union: Art. 26 [Online, zitiert am 2017-01-02] Verfügbar unter https://dejure.org/gesetze/AEUV/26.html

Innerhalb der Europäischen Union oder des EWR (die Länder der EU sowie Island, Liechtenstein und Norwegen) existiert ein vergleichbar hohes Datenschutzniveau, sodass ein AV-Vertrag entsprechend deutschem Recht abgeschlossen werden kann.

Außerhalb der EU / des EWR ist eine Beauftragung unter folgenden Voraussetzungen möglich:

Eine Beauftragung von Auftragnehmern in Ländern, denen die Europäische Kommission bereits ein angemessenes Datenschutzniveau attestiert hat, sog. sichere Drittstaaten, ist rechtlich zulässig; die Liste der Länder steht online zur Verfügung[27].

Bei sog. Drittländern (= Land ohne ein als hinreichend anerkanntes Datenschutzniveau) ist gemäß Art. 44 DS-GVO ebenfalls die Sicherstellung eines angemessenen Datenschutzniveaus beim Datenempfänger zu gewährleisten. Um dies zu bewerkstelligen, hat die Europäische Kommission sogenannte „Standardvertragsklauseln“ bereitgestellt, welche beim Einsatz eines Auftragsverarbeiters in einem solchen Drittland verwendet werden müssen, wenn unter dem Aspekt der Auftragsverarbeitung 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.[28] Die Rechte und Pflichten der Parteien werden geregelt und müssen unverändert übernommen werden. 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.

Entsprechend Art. 49 DS-GVO sind auch Ausnahmen möglich, in denen personenbezogene Daten in ein Drittland ohne angemessenes Datenschutzniveau transportiert werden dürfen.

Standardvertragsklauseln der Kommission („EU-Standardvertrag“)

Die derzeit geltenden Standardvertragsklauseln[29] behalten entsprechend ErwGr. 171 ihre Gültigkeit, bis sie entweder von der Kommission oder dem EuGH für ungültig erklärt werden.

Bei Nutzung der Standardvertragsklauseln muss beachtet werden, dass dieser Vertrag immer zwischen Datenexporteur (dem eigentlichen Auftraggeber) und Datenimporteur (also die Stelle im Drittland) geschlossen werden. Dies gilt auch, wenn der Datenimporteur als Unterauftragnehmer eines innerhalb der EU tätigen Auftragnehmers auftritt. D.h. die „klassische“ Vertragskonstellation bei Einschaltung eines Unterauftragnehmers ist in diesem Fall nicht gegeben, vielmehr existiert dann eine direkte Vertragsbeziehung zwischen Auftraggeber und Unterauftragnehmer. In

[27] Commission decisions on the adequacy of the protection of personal data in third countries. [Online, zitiert am 2017-02-11] Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[28] Bzgl. Möglichkeiten der Verarbeitung von Daten in einem Drittland siehe Artt. 44-50 EU DS-GVO sowie entsprechende Kommentierungen

[29] EU-Kommission: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. [Online, zitiert am 2016-05-26]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445851652852&uri=CELEX:32010D0087

der Praxis findet sich oftmals die Gestaltung, dass sich der Auftragnehmer vom Auftraggeber die Befugnis geben lässt, dass der Auftragnehmer im Namen des Auftraggebers einen EU-Standardvertrag mit einer in einem Drittland ansässigen datenverarbeitenden Stelle abschließt.

Weiterhin ist bei Nutzung der Standardvertragsklauseln zu beachten, dass in Klausel 4 die Pflichten des Datenexporteurs (= Auftraggeber) beschrieben werden, in Klausel 5 die des Datenimporteurs (= Stelle im Drittland).

Der Datenexporteur verpflichtet sich bei Vertragsabschluss u.a. dazu, dass

- er den Datenimporteur auswählte, weil dieser hinreichende Garantien bzgl. der Sicherheit der personenbezogenen Daten gewährleistet,
- er für die Einhaltung der Sicherheitsmaßnahmen beim Datenimporteur sorgt,
- er die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis setzt, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau bietet
- er der betroffenen Person auf Anfrage eine Kopie des Vertrags mit Ausnahme sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt

Bei Anwendung der vorliegenden Standardvertragsklausen garantiert der Datenimporteur insbesondere, dass

- 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,
- er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

Auftragsverarbeitung in den USA

Die EU-Kommission veröffentlichte am 29. Februar 2016 die Unterlagen bzgl. des „Privacy Shield“ genannten bilateralen Abkommens zwischen den USA und der EU[30]. Am 08. Juli 2016 einigten sich die EU-Mitgliedsstaaten im Rahmen der Beratungen des sog. Art.-31-Ausschusses mehrheitlich auf die Annahme des Textes[31]. Damit soll ein rechtssicherer Ersatz für das vom EuGH für ungültig erklärte Safe Harbor Abkommen zur Verfügung gestellt werden.

Es gibt schon heute eine Vielzahl von Stimmen, welche die Meinung vertreten, dass das Privacy-Shield-Abkommen den aus dem EuGH-Safe-Harbor-Urteil resultierenden Anforderungen auch nicht gerecht wird. Die Kommission hat dennoch die Möglichkeit, das Privacy-Shield-Abkommen als Rechtsmittel anzuerkennen, was am 08. Juli 2016 ja auch geschah. Entsprechend dem Safe-Harbor-Urteil kann abgesehen von der EU-Kommission selbst nur der EuGH diese Anerkennung aufheben. D. h. solange dies nicht geschieht, ist das Privacy-Shield-Abkommen als legales Mittel anzusehen. Es gibt auch einen offiziellen Leitfaden zum Umgang mit

[30] Europäische Kommission - Pressemitteilung zur Veröffentlichung (inkl. Link zu Texten) [Online, zitiert am 2017-01-27] Verfügbar unter http://europa.eu/rapid/press-release_IP-16-433_de.htm

[31] European Commission: The EU-U.S. Privacy Shield. [Online, zitiert am 2017-01-27] Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

dem Privacy-Shield-Abkommen, der in allen Sprachen der EU Mitgliedsländer verfügbar ist[32].
Die US-Regierung richtete eine eigene Webseite[33] zum Privacy-Shield-Abkommen ein, auf welcher u. a. auch die Unternehmen gelistet sind, die sich zur Einhaltung der Regelungen des Privacy Shields verpflichteten.

Literatur

(1) Eckhardt J, Kramer R. (2016) Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools. DuD: 144-149
(2) Koós C, Englisch B. (2014) Eine "neue" Auftragsdatenverarbeitung? - Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs. ZD: 276-285
(3) Müthlein T. (2016) ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 74-87
(4) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
(5) Schmitz B, von Dall'Armi J. (2016) Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? - Wie Daten künftig von Dienstleistern verarbeitet werden müssen. ZD: 427432
(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

[32] Leitfaden zum EU-US-Datenschutzschild, deutsche Fassung. [Online, zitiert am 2017-01-27] Verfügbar unter http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf
[33] U.S. Department of Commerce: Privacy Shield Overview.) [Online, zitiert am 2017-01-27] Verfügbar unter https://www.privacyshield.gov

§ 7 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 Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich 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 erfolgt im Anlage 2 zu diesem Vertrag.

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

(4) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

Opt. (6) Die Wahrung des Fernmeldegeheimnisses entsprechend §88 TKG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf Daten des Auftraggebers mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.

(7) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

Opt. (8) 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.

(9) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit _____ [*Name, Kontaktdaten*] benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(10) 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 der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Artt. 33, 34 DS-GVO.

(11) 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.

(12) 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.

(13) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person 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.

(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 Auftraggeber bestätigt oder geändert wird.

(16) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.

(17) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.

Alt. 1 zu Opt. Abs. 18

(18) Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen.

Alt. 2 zu Opt. Abs. 18

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

(19) Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

(20) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

Kommentierung § 7

Artt. 28 bis 33 DS-GVO schreiben einige Pflichten des Auftragnehmers vor, andere ergeben sich aus dem allgemeinen Datenschutzrecht, den landesrechtlichen Bestimmungen wie auch aus dem Haftungsrecht.

Datenschutz-Folgenabschätzung

Die Verarbeitung von besonderen Kategorien von Daten entsprechend Art. 9 DS-GVO beinhaltet i. d. R. ein vergleichsweise hohes Risiko für die Rechte und Freiheiten natürlicher Personen, sodass bei Verarbeitungsvorgängen eine Datenschutz-Folgenabschätzung entsprechend Art. 35 DS-GVO vorzunehmen ist. Ggf. resultiert daraus, dass vor der Verarbeitung eine Konsultation der zuständigen Aufsichtsbehörde entsprechend Art. 36 DS-GVO erforderlich wird. Bei beiden Pflichten des Auftraggebers ist der Auftragnehmer zur Unterstützung dahingehend verpflichtet, dass der Auftragnehmer dem Auftraggeber alle ihm selbst zur Verfügung stehenden Informationen zur Verfügung stellt.

Technisch-organisatorische Maßnahmen

Die eigentlichen technisch-organisatorischen Maßnahmen (TOMs), welche der Auftragnehmer zum Schutz der ihm anvertrauten Daten trifft, können in einem Anhang (Opt. unter Abs. 2) dargestellt werden. Hier wird vertraglich festgehalten, dass der Auftragnehmer die Vorschriften der DS-GVO berücksichtigt und einhält sowie dem Auftraggeber nachweist (§ 3 Ziff. (2)).

Der Gesetzgeber schreibt vor, dass der Auftragnehmer hinreichende Garantien dafür bieten muss, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet, nicht jedoch, wie dies genau zu geschehen hat. Art. 32 Abs. 1 DS-GVO gibt allerdings Rahmenbedingungen vor, die einzuhalten sind. Insbesondere muss der Stand der Technik berücksichtigt werden, aber auch die Implementierungskosten sowie die Eintrittswahrscheinlichkeit einer Datenpanne und das Risiko für die betroffene(n) Person(en).

Der Auftraggeber muss ggf. der Aufsichtsbehörde gegenüber den Auswahlprozess und die diesbezüglich zugrundeliegenden Beurteilungskriterien nachweisen. Daher darf bzgl. des Nachweises, wieso der Auftragnehmer aus Sicht des Auftraggebers für die Verarbeitung geeignet ist, keine Beschränkung durch den Auftragnehmer erfolgen. Eine Beschränkung von Seiten des Auftragnehmers auf eine ausschließliche Beurteilung auf der Grundlage von Zertifikaten wäre beispielsweise unzulässig. (Abgesehen davon hätte speziell diese Regelung den Nachteil, dass der Auftragsverarbeitungsprozess 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 erforderlichen Maßnahmen, so kann dies die Datenverarbeitung durch den Auftragnehmer rechtswidrig machen. Daher müssen die TOMs entsprechend den sich wandelnden Gegebenheiten angepasst werden können, ohne

dass damit der Vertrag als solches geändert werden müsste. Daher wird in § 3 Zeilen 13-18 des Muster-AV-Vertrages genau auf diesem Umstand hingewiesen.

Datenschutzbeauftragter

Der Auftrag darf nur erteilt werden, wenn bei Vorliegen einer gesetzlichen Benennungspflicht beim Auftragnehmer ein ordentlich benannter Datenschutzbeauftragter vorhanden ist, welcher dem Auftraggeber namentlich mitgeteilt werden muss (§ 7 Ziff. 8).

Als fachliche Voraussetzungen verweist die DS-GVO in Art. 37 Abs. 5 insbesondere auf das Fachwissen, das der Datenschutzbeauftragte auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie die Fähigkeit, seine Aufgaben gemäß Art. 39 DS-GVO zu erfüllen.

Die Artikel-29-Datenschutzgruppe veröffentlichte am 13.12.2016 eine Leitlinie sowie ein FAQ bzgl. des Themas „Datenschutzbeauftragter“[34]. Die Artikel-29-Datenschutzgruppe geht in dieser Leitlinie u. a. auf die Bestellpflicht ein, Da in sämtlichen bisher bekannt gewordenen Entwürfen für das Nachfolgegesetz des BDSG an der aktuell in Deutschland geltenden Bestellpflicht festgehalten wird, greift die deutsche Bestellpflicht früher als die DS-GVO, so dass diese Empfehlungen für Deutschland wohl nicht anwendbar sind; abgesehen vielleicht von der Empfehlung, die Überlegungen zur Benennungspflicht bzw. Nicht-Benennung bei der jeweiligen Stelle zu dokumentieren. Bzgl. der fachlichen Qualifikation werden einerseits ausgewiesene Kenntnisse im nationalen und europäischen Datenschutzrecht sowie insbesondere der DS-GVO verlangt, andererseits bzgl. des Wissens in technischen Angelegenheiten ein ausreichendes Verständnis der Verarbeitungstätigkeiten vorausgesetzt; die Artikel-29-Datenschutzgruppe stellt zugleich klar, dass sich die Anforderungen an den Datenschutzbeauftragten je nach Unternehmen und Branche unterscheiden können.

Der Düsseldorfer Kreis veröffentlichte die Mindestanforderungen an Fachkunde und Unabhängigkeit eines Datenschutzbeauftragten[35]. 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[36]. Darin werden z. T. Anforderungen beschrieben, die über die Ansprüche des Düsseldorfer Kreises hinausgehen. Es orientiert sich sowohl an den verpflichtenden Aufgaben gemäß DS-GVO, beschreibt aber auch Aufgaben, bei denen der Datenschutzbeauftragte die Verantwortlichen unterstützen kann. Es ist wünschenswert, dass der Datenschutzbeauftragte des Auftragnehmers dem beruflichen Leitbild des BvD genügt; für die Auftragsvergabe ist dies jedoch keine zwingende Voraussetzung.

[34] Article 29 Working Party: Guidelines and FAQs on Data Protection Officers (DPO). [Online] 2016 [Zitiert 2017-02-11] Verfügbar unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[35] 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

[36] Berufsverband der Datenschutzbeauftragten Deutschlands: Berufliches Leitbild der Datenschutzbeauftragten). [Online] 2016 [Zitiert 2016-12-02] Verfügbar unter https://www.bvdnet.de/berufsbild.html

Sofern keine gesetzliche Benennungspflicht besteht, ist die freiwillige Benennung eines Datenschutzbeauftragten in Anbetracht der Sensibilität der Daten, der gesetzlichen Kontroll-, Prüf- und Dokumentationspflichten sowie der evtl. durchzuführenden Datenschutzfolgeabschätzung empfehlenswert. Zwingend muss aber dem Auftraggeber ein kompetenter Ansprechpartner benannt werden.

Mitteilung bei Verstößen

Der Auftragnehmer muss den Auftraggeber über Missachtungen bzgl. der vertraglich vereinbarten Leistungen bzw. über datenschutzrechtliche Verstöße informieren (§ 7 Ziff. 9), damit der Auftraggeber seiner gesetzlichen Verpflichtung bzgl. Benachrichtigung des Betroffenen bzw. Mitteilung an die 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. 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). Unter der Maßgabe, dass unter der DS-GVO ähnliche Regelungen vorhanden sind und die Rechtsprechung bestehen bleibt, gilt auch weiterhin: Für einen entsprechenden Hinweis darf der Auftragnehmer daher nicht warten, bis er sichere Kenntnis von der Rechtswidrigkeit hat. Betrifft der Auftrag besonders sensible Daten wie Gesundheitsdaten, so ist der Auftragnehmer zudem zu einer erhöhten Aufmerksamkeit verpflichtet.

Die Verantwortlichkeit des Auftraggebers bedingt, dass er bei unsicherer Rechtslage grundsätzlich die Erfüllung seiner Weisung durch den Auftragnehmer verlangen kann. Der Auftragnehmer hat nur das Recht, die Durchführung einer Weisung zu verweigern, wenn

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

§ 7 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 ggf. rechtswidrige Verarbeitung durchzuführen.

Verpflichtung des vom Auftragnehmer eingesetzten Personals

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 § 7 Ziff. 6 TKG ist.

Das Gesetz gegen den unlauteren Wettbewerb (UWG) setzt in § 17 den Verrat von Geschäfts- und Betriebsgeheimnissen unter Strafe. Neben den üblichen Geschäfts-

und Betriebsgeheimnissen sind auch die während der Tätigkeit für den Auftraggeber vom Auftragnehmer erlangten Patientendaten 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. Daher wird im Muster AV-Vertrag die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen gefordert (§ 7 Ziff. 7).

Ersuchen eines Betroffenen auf Berichtigung und Löschung von Daten

Betroffene haben grundsätzlich das Recht auf Berichtigung, Einschränkung der Verarbeitung (bisherige Begrifflichkeit „Sperrung“) und Löschung der Daten. Im Rahmen einer Auftragsverarbeitung bleibt jedoch der Auftraggeber dem jeweiligen Betroffenen gegenüber verantwortlich, sodass nur der Auftraggeber den Auftragnehmer mit der Einleitung entsprechender Maßnahmen beauftragen kann (§ 7 Ziff. 12).

Für den Fall, dass sich ein Betroffener direkt an den Auftragnehmer wendet, wird vertraglich festgehalten, wie damit umzugehen ist (§ 7 Ziff. 10). 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 (§ 7 Ziff. 12).

Gesetzliche Offenbarungspflicht

Gesetzliche Offenbarungspflichten können für den Auftragnehmer beispielsweise aus

- Nichtanzeige geplanter (besonders schwerer) Straftaten wie Mord oder Totschlag, erpresserischen Menschenraub oder Geiselnahme (§ 138 StGB bzw. § 139 StGB)
- § 34 StGB rechtfertigendem 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 sollte ausschließlich beim Auftraggeber stattfinden. In einem (zu begründenden) Einzelfall kann es entsprechend den landesrechtlichen Bestimmungen dennoch notwendig sein, dass Daten nur beim Auftragnehmer gespeichert und verarbeitet werden.

Für diesen Fall müssen bzgl. des Umgangs bei Gefahr einer Beschlagnahme oder Pfändung der Daten des Auftragnehmers vertragliche Regelungen getroffen werden (§ 7 Ziff. 15).

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 befinden oder
c) eines Dienstleisters, der für den Arzt bzw. die Institution personenbezogene Daten erhebt, verarbeitet oder nutzt (§ 97 Abs. 2 S. 2 StPO).

Ohne einen rechtswirksamen AV-Vertrag wird man wohl davon ausgehen müssen, dass bei einem Dienstleister kein Beschlagnahmeverbot gilt. Bzgl. der Rechtskonformität eines AV-Vertrages muss ggfs. auch die Diskussion bzgl. der gesetzlich vorgeschriebenen Schweigepflicht (siehe Kapitel 4.5) berücksichtigt werden.

§ 7 sieht in Abs. 17 als optionale Regelung vor, dass der Auftragnehmer keine Patientendaten auf Systemen speichert, die außerhalb der Verfügungsgewalt des Auftraggebers liegen und als weitere Alternative, dass der Auftragnehmer keine Patientendaten auf Systemen speichert, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen. Durch eine solche Regelung soll sichergestellt werden, dass eine Datenverarbeitung außerhalb der Verfügungsgewalt des Auftraggebers bzw. in Ländern, in denen kein Beschlagnahmeschutz beim Auftragnehmer besteht, ausgeschlossen ist. Diese Regelung ist zu streichen, sofern dies je nach Fallgestaltung technisch nicht möglich sein sollte.

Datenschutzverstöße beim Auftragnehmer

Der Auftraggeber ist und bleibt im Rahmen einer Auftragsverarbeitung „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 (§ 7 Ziff. 9 und 13), dies gilt sowohl für auftretende Datenschutzverstöße wie auch für beim Auftragnehmer stattfindende Kontrollen durch Aufsichtsbehörden.

Auskunft durch den Auftraggeber

Der Auftraggeber muss auf Nachfrage den betroffenen Personen über Art und Umfang der Verarbeitung seiner Daten informieren. Dabei ist der Auftraggeber ggf. 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 AV-Vertrag verankern (§ 3 Ziff. 12).

Zweitnutzung der Daten durch den Auftragnehmer

Die DS-GVO stellt ausdrücklich fest, dass Daten nur auf dokumentierte Weisung des Auftraggebers verarbeitet werden dürfen. Dies schließt jegliche eigenständige Verarbeitung der Daten zu Zwecken des Auftragnehmers aus.

Verarbeitet ein Auftragnehmer Daten des Auftraggebers zu eigenen Zwecken oder bestimmt eigenständig und unabhängig vom Auftraggeber die Mittel der Verarbeitung, so wird er dadurch entsprechend Art. 28 Abs. 10 DS-GVO in Bezug auf diese Verarbeitung selbst Verantwortlicher. Dies beinhaltet eine Datenweitergabe vom Auftraggeber an den Auftragnehmer, welche einen Erlaubnistatbestand im Sinne von Art. 9 DS-GVO benötigt. Um dies zu vermeiden, muss dem Auftragnehmer eine entsprechende eigenständige Verarbeitung vertraglich untersagt werden.

Zuständige Aufsichtsbehörde

Grundsätzlich können sowohl Auftragnehmer als auch Auftraggeber durch die zuständige Aufsichtsbehörde kontrolliert werden, obwohl bzgl. des konkreten Umgangs mit personenbezogenen Daten zunächst der Auftraggeber Adressat aufsichtsbehördlicher Maßnahmen sein dürfte. Maßnahmen beim Auftragnehmer sind jedoch auch immer möglich.

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 2017-02-23]; 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) Müthlein T. (2016) ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 74-87
7) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
8) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

Opt. § 8 Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.

(2) Fernzugriffe im Rahmen von 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 werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von 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 Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie 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 solchem 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 im Rahmen von 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 § 8

Fernwartung/Fernservice

In der Praxis kann es sinnvoll sein, nicht nur die Wartung, sondern auch umfangreiche Dienstleistungen bis hin zum kompletten Betrieb einer Datenverarbeitungsanlage über eine Fernverbindung durchführen zu lassen (Remote Services). In diesem Fall ist der Vertragstext entsprechend anzupassen.

Bei umfangreichen Dienstleistungen über Fernzugriffe sollte ein Sicherheitskonzept zwischen Auftraggeber und Auftragnehmer vereinbart werden, auf das an dieser Stelle verwiesen werden kann. (Anlage zu den technischen und organisatorischen Maßnahmen)

Verfügungsgewalt der Krankenhäuser

Einige krankenhausspezifische landesrechtliche Regelungen sehen vor, dass die Daten in der Verfügungsgewalt der Krankenhäuser verbleiben müssen bzw. nur im Krankenhaus selbst verarbeitet werden dürfen.

Im Falle der Beauftragung von (Fern-) Wartungstätigkeiten lässt sich diese Anforderung dahingehend lösen, dass moderne Maßnahmen wie ein Remote Desktop eine Fernwartung erlauben, 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[37] bzgl. Streaming, bei welchem ein Film oder Musikstück ja nie vollständig beim Anwender gespeichert werden (analog wie beim Fernwartenden nie alle Daten gespeichert werden), so wird entsprechend der Rechtsprechung des EuGH durch diese Maßnahme keine Kopie der Patientendaten erstellt. Somit behält der Auftraggeber die Hoheitsgewalt über die Daten, was den Vorgaben vieler Krankenhausgesetze genügt. Ist man der Auffassung, dass die Analogie nicht auf die Fernwartung übertragbar ist, muss man ggf. davon ausgehen, dass eine Fernwartung evtl. nicht zulässig ist und eine Wartung nur vor Ort durchführbar ist.

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 wartenden System, ist aber aus strafrechtlichen Gesichtspunkten zu fordern.

Protokollierung

Da Protokolldaten geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sollten Mitbestimmungsrechte der Personalvertretungen berücksichtigt werden (vgl. § 87 Abs. 1 Nr. 6 BetrVG). Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ist weit gefasst und setzt bereits dann ein, wenn eine technische Einrichtung zur Verhaltens- und Leistungskontrolle auch nur abstrakt geeignet ist. Auf ein konkretes Kontrollinteresse von Arbeitgebern kommt es hingegen nicht an. Deshalb ist die frühzeitige Beteiligung der Personalvertretung und

[37] z. B. EuGH Urteil vom 05.06.2014 AZ: C-360/13 [Online, zitiert am 2016-12-26]; Verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=153302&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

des/der Datenschutzbeauftragten vor der Einführung einer Protokollierung von Mitarbeiterdaten anzuraten.

Der Europäische Gerichtshof für Menschenrechte wies in einem Urteil aus dem Jahr 2008 darauf hin, dass im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems in einer fehlenden Protokollierung von Zugriffen auf medizinische Daten ein Verstoß gegen Art. 8 der Europäischen Menschenrechtskonvention vorliegen kann[38]. Ggf. sollte gegenüber der Personalvertretung daher auch ein Hinweis erfolgen, dass rechtliche Erfordernisse eine Protokollierung bedingen, man sich letztlich nur auf eine rechtskonforme Auswertung der Protokollierung einigen muss.

Angemessene Identifizierungs- und Verschlüsselungsverfahren

Das Bundesamt für Sicherheit in der Informationstechnik veröffentlichte eine technische Richtlinie bzgl. kryptographischer Verfahren, die auch Empfehlungen zur Schlüssellänge enthält[39]. In Teil 4 der Richtlinie („Kommunikationsverfahren in Anwendungen“) widmet sich Kapitel 5 der sicheren Identifizierung von Kommunikationspartnern, so dass die Richtlinie neben der Wahl der Verschlüsselungsverfahren sowie der Schlüssellängen auch bzgl. der Frage eines sicheren Identifizierungsverfahrens unterstützt.

Entsprechend der Orientierungshilfe der Datenschutzaufsichtsbehörden[40] ist die „Wahl der Verschlüsselungsverfahren und deren Parameter unter dem Aspekt des angemessenen Aufwands zu betrachten“. Entsprechend der Orientierungshilfe ist bei der Betrachtung des Aufwands die Marktsituation bzgl. der Möglichkeit der Beschaffung von Produkten, die mit geeigneten Schlüssellängen operieren können, ausschlaggebend. D. h. Angemessenheit liegt vor, wenn auf dem Markt auch nutzbare Produkte vorliegen.

Literatur

(1) Bartsch M. (2012) Softwarerechte bei Projekt- und Pflegeverträgen. CR: 141-146

(2) Bohnstedt J. (2015) Fernwartung: Die rechtlichen Grenzen des IT-Outsourcing durch Banken. Nomos Verlagsgesellschaft, 1. Auflage. ISBN 978-3-83291-325-0

(3) Fischer A. (2011) Wartungsverträge: Inspektion, Wartung und Instandsetzung technischer Einrichtungen. Erich Schmidt Verlag, 3. Auflage. ISBN 978-35-03129-98-0

(4) Hartung J, Stiemerling O. (2011) Effektive Service-Level-Kriterien - Welche Service Level-Kriterien effektiv sind und wie sie gemessen und vertraglich geschickt vereinbart werden können. CR: 617-624

[38] EGMR, Urteil vom 17.07.2008, AZ 20511/03 R: 44 „It is plain that had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. [Online, zitiert am 2017-01-29]; Verfügbar unter http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87510

[39] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2016) BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Online, zitiert am 2017-01-29]; Verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[40] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2003) Orientierungshilfe zum Einsatz kryptografischer Verfahren. [Online, zitiert am 2017-01-28]; Verfügbar unter https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHEinsatzKryptografischerVerfahren.pdf?__blob=publicationFile&v=5

(5) Hörl B. (2010) Auswirkungen der InvMaRisk auf IT-Outsourcingverträge. ITRB: 217-219
(6) Hörl B, Braun S. (2016) Gestaltung von Pflegeverträgen für Individualsoftware - Vertragliche Unterschiede zur Standardsoftwarepflege aus Anbieter- und Anwendersicht. ITRB: 256-260
(7) Intveen M. (2001) Fernwartung von IT-Systemen - Wie kann bzw. muss sich der Anwender vor einem Zugriff auf sensible Datenbestände schützen? ITRB: 251-252
(8) Intveen M. (2015) Verträge über Einrichtung, Betrieb und Wartung von Telekommunikationssystemen ITRB: 262-265
(9) Intveen M. (2015) Der EVB-IT Servicevertrag - Serviceleistungen aus einem Vertrag. ITRB: 47-50
(10) Kremer S, KammK. (2013) Absicherung der (Re-)Migration beim IT-Outsourcing. ITRB: 264-267
(11) Ortner G. (2015) Projektmanagement-Outsourcing. Springer Verlag, 1. Auflage. ISBN 978-3-662-45009-3
(12) Osterheider G. (2015) Der Service as before-Grundsatz im Outsourcingvertrag. ITRB: 124-126
(13) Schultze-Melling J. (2005) Effizientes Information Security Management im Rahmen von IT-Outsourcing-Verträgen. ITRB: 42-46
(14) Schumacher V. (2006) Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen. MMR: 12-17
(15) Schuster F. (2009) Rechtsnatur der Service Level bei IT-Verträgen - Wie die Gestaltung von Service Levels die Leistung, die Gewährleistung und den Vertragstyp konkretisiert. CR: 205-210
(16) Siebenhüner R. (2013) Wartung technischer Systeme im Krankenhaus durch externe Dienstleister. Deutsche Krankenhaus Verlagsgesellschaft, 1 Auflage. ISBN 978-3-942734-49-3
(17) Söbbing T. (2013) Transition und Transformation im IT-Outsourcingprojekt - Rechtsfragen zu Übergabe und Erneuerung von IT-Services im Rahmen des Outsourcings. ITRB: 93-95

§ 9 Pflichten des Auftraggebers

(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 für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(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 – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Dem Auftraggeber obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

(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. (7) Weiterhin sind alle Personen des Auftraggebers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftragnehmers zu verpflichten und müssen auf §17 UWG hingewiesen werden.

(8) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

Opt. (9) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

Kommentierung § 9

Art. 28 DS-GVO regelt die datenschutzrechtliche Verantwortung des Auftraggebers im Rahmen der Auftragsverarbeitung. Entsprechend können einige daraus resultierende Pflichten nicht vom Auftragnehmer übernommen werden, sondern obliegen dem Auftraggeber. Insbesondere muss der Auftraggeber dafür Sorge tragen, dass im Rahmen seiner technischen und organisatorischen Maßnahmen die Sicherheit der Verarbeitung gewährleistet ist. D. h., dass beispielsweise auch beim Auftraggeber der Stand der Technik bei einer Verarbeitung während eines Fernzugriffs gewahrt werden muss.

Verantwortlicher

Verantwortlicher im Sinne des Datenschutzrechts bleibt der Auftraggeber (§ 3 Ziff. 1). Desgleichen kann der Auftraggeber auch nicht andere, höchstpersönliche Pflichten an den Auftragnehmer weiterreichen.

Daraus resultiert auch, dass der Auftraggeber z. T. für die beim Auftragnehmer stattfindende Datenverarbeitung datenschutzrechtlich verantwortlich bleibt (§ 3 Ziff. 4) und das für ihn geltende Verzeichnis von Verarbeitungstätigkeiten führen muss.

Die Verantwortlichkeit des Auftraggebers besteht auch hinsichtlich der Rechte der Betroffenen (Artt. 12-22 DS-GVO), welche die Betroffenen gegenüber dem Auftragnehmer geltend machen können. Zusätzlich haben Betroffene, sofern die entsprechenden tatbestandlichen Voraussetzungen vorliegen, einen eigenständigen (Haftungs-) Anspruch gegen den Auftragnehmer. Die Verantwortlichkeit des Auftragnehmers gegenüber den Betroffenen ist dabei losgelöst von der Frage nach einer Haftung des Auftragnehmers gegenüber dem Auftraggeber im Innenverhältnis (siehe § 9 bzw. entsprechende Kommentierung) zu sehen.

Kontrollpflichten des Auftraggebers

Siehe Kommentierung § 1

Informationspflichten des Auftraggebers

Der Gesetzgeber sieht vor (Art. 34 DS-GVO), dass ein Verantwortlicher (oder auch mehrere Verantwortliche) einen Betroffenen bei einer Verletzung des Schutzes seiner Daten gegebenenfalls informieren muss. Diese Pflicht bleibt beim Auftraggeber als für die Daten Verantwortlicher (§ 3 Ziff. 4). Je nach erteilter Weisung gelten für den Auftraggeber neben den aus der DS-GVO resultierenden Pflichten auch die Informationspflichten aus dem Telemediengesetz.

Verpflichtung nach §17 UWG

siehe Abschnitt „Verpflichtung des vom Auftragnehmer eingesetzten Personals“ in der Kommentierung § 7 auf Seite 55

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 (§ 9 Opt. 9). Diese Regelung

ist gesetzlich nicht gefordert, entspricht aber den Gepflogenheiten zwischen Vertragsparteien. Allerdings empfiehlt sich diesbezüglich eine entsprechende schriftliche Vereinbarung über die Kosten.

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

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und –prüfzeichen berücksichtigen,
- schriftliche Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen oder
- sich 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 der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

(3) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber 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.

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

Kommentierung § 10

Der Gesetzgeber fordert vom Auftraggeber, dass er nur Auftragnehmer auswählt, die hinreichende Garantien für die Einhaltung der Datenschutzvorschriften bieten. Daher muss der Auftraggeber vor Abschluss des AV-Vertrages die Einhaltung der im AV-Vertrag vereinbarten Pflichten des Auftragnehmers prüfen[41] und das Ergebnis der Prüfung dokumentieren (§ 10 Ziff. 1)[42]. Entsprechend Art. 83 Abs. 5 lit. a DS-GVO 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[43] zu informieren (§ 10 Ziff. 4), damit der Auftragnehmer diese beseitigen kann. Da der Auftraggeber verantwortlich für die beim Auftragnehmer durchgeführte Datenverarbeitung ist, liegt die Beseitigung festgestellter Mängel im Interesse des Auftraggebers. Da der Aufragnehmer jedoch auch für die durch ihn durchgeführte Verarbeitung haftet, wenn diese nicht den Weisungen des Auftraggebers entspricht, liegt die Beseitigung/Vermeidung einer fehlerhaften Verarbeitung auch in seinem Interesse.

Um Prüfungen hinsichtlich der auftragskonformen Verarbeitung zu ermöglichen und damit seinen gesetzlichen Verpflichtungen nachzukommen, muss der Auftragnehmer vertraglich dazu verpflichtet werden, diese Prüfungen zu unterstützen (§ 10 Ziff. 3), d. h. dem Auftraggeber entsprechende Rechte einzuräumen. Ohne eine vertraglich vereinbarte Unterstützungspflicht des Auftragnehmers ist der Auftraggeber ggf. nicht in der Lage, entsprechende Kontrollen durchzuführen.

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 sein, da hierbei ein Umstand vorliegt, der ggf. 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 (§ 10 Ziff. 2).

Überprüfung des Auftragnehmers

Auch wenn eine fortdauernde Überprüfungspflicht des Verantwortlichen nicht explizit in Art. 28 DS-GVO hineingeschrieben wurde, ergibt sich diese aus Art. 28 Abs. 1 DS-GVO[44]: der Verantwortliche darf nur mit Auftragsverarbeitern arbeiten, welche den Erfordernissen der DS-GVO entsprechen. Es wird der gesamte

[41] 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

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

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

[44] siehe hierzu bspw. auch Martini M. Art. 28. Rn. 21 in Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag 1. Auflage. ISBN 978-3-406-69570-4

Verarbeitungszeitraum angesprochen, nicht nur der Zeitpunkt der Auswahl. Daher bleibt es dabei, dass der Verantwortliche sich fortwährend vergewissern muss, dass der Auftragsverarbeiter die durch Art. 28 Abs. 1 DS-GVO genannten Anforderungen erfüllt.

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
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

§ 11 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

(2) Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Haupt-Vertrag bereits eine entsprechende Regelung getroffen worden ist.

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

Alt. 1 zu Abs. 4

(4) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Alt. 2 zu Abs. 4

(4) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Alt. 3 zu Abs. 4

(4) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer

a. sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b. erstellte Verarbeitungsergebnisse,

dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Alt. 4 zu Abs. 4

(4) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer

a. sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b. erstellte Verarbeitungsergebnisse,

c. Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen

dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Alt. 1 zu Abs. 5

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

Alt. 2 zu Abs. 5

(5) Sofern der Aufwand der Löschung gesondert vergütet werden soll, ist hierüber eine gesonderte schriftliche Vereinbarung zu treffen.

Alt. 3 zu Abs. 5

(5) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

(6) 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.

(7) 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.

(8) Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

(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 anders 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) 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. (11) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

Kommentierung § 11

Es ist vorgeschrieben (Art. 28 Abs. 3 lit. g DS-GVO), dass der AV-Vertrag Regelungen bzgl. Art und Weise der gesetzlich geforderten Löschung oder Rückgabe von Daten, Datenträgern usw. für den Zeitpunkt nach Abschluss der Erbringung der Verarbeitungsleistungen enthalten muss. Daher muss die Löschung bzw. Rückgabe der Daten unabhängig vom Weisungsrecht des Auftraggebers vertraglich abgebildet werden. Hierbei können - unabhängig von der gesetzlichen Forderung - auch weitergehende Daten berücksichtigt werden. Daher werden vier alternative Regelungen vorgestellt.

Gesetzlich nicht verpflichtend im AV-Vertrag zu regeln, aber empfehlenswert sind entsprechende Regelungen für die Zeit der laufenden Beauftragung.

Über das Vertragsende hinaus kann der Nachweis der Erbringung der vertraglich geschuldeten Leistungen seitens des Auftragnehmers aufzubewahren sein. Hier nur der Hinweis, dass z. B. Bestell- und Auftragsunterlagen einer gesetzlichen Aufbewahrungsfrist von derzeit 6 Jahren unterliegen. Weitere Beispiele finden sich z. B. im Leitfaden der Deutschen Krankenhausgesellschaft zu Aufbewahrungspflichten und –fristen von Dokumenten im Krankenhaus[45]. Daher wird im Vertrag geregelt, dass derartige Unterlagen vom Auftragnehmer bis zum Ablauf der einschlägigen Aufbewahrungsfristen nicht gelöscht werden dürfen (§ 9 Ziff. (7)).

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

[45] Deutsche Krankenhausgesellschaft e.V. (2015) Leitfaden Aufbewahrungspflichten und –fristen von Dokumenten im Krankenhaus, Stand: September 2015. [Online, zitiert am 2017-02-11]; Verfügbar unter http://www.dkgev.de/dkg.php/cat/133/aid/13847/title/DKG-Leitfaden_Aufbewahrungspflichten_und_-fristen_von_Dokumenten_im_Krankenhaus_____Zurverfuegungstellung_einer_erneut_aktualisierten_Fassung_des_DKG-Leitfadens_%28Stand%3A_September_2015%29

§ 12 Unterauftragnehmer

Alt 1 Unterauftragsverhältnisse nicht erlaubt

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

Alt 2 Unterauftragsverhältnisse erlaubt

(1) Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch Unterauftragnehmer begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

(2) Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

(3) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

Alt. 1 zu Opt. Abs. 5

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung werden die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Leistungsteile unter Einschaltung eines Unterauftragnehmers durchgeführt, nämlich

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen

Alt. 2 zu Opt. Abs. 5

(5) 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.

(6) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(7) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

(8) 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.

(9) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei 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.

(10) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

Kommentierung § 12

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 den Einbezug von Unterauftragnehmern ausdrücklich zu, verlangen aber, dass diese Verhältnisse im AV-Vertrag geregelt werden.

Unter dem Aspekt, dass der Gesetzgeber fordert, dass bei einem AV-Vertrag der Auftraggeber stets „Herr der Daten“ bleibt, muss 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.

Eine generelle schriftliche Erlaubnis des Auftraggebers zu einer beliebigen Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist rechtlich zulässig, aber auch hierbei muss entsprechend Art. 28 Abs. 2 DS-GVO der Auftragnehmer den Auftraggeber über jede Hinzuziehung oder Ersetzung von Unterauftragnehmern informieren, wobei der Auftraggeber jeweils ein Widerspruchsrecht hat (§ 12 Alt. 2 von Ziff. 2). Eine Zustimmung sollte der Auftraggeber jedoch nur aus wichtigen Gründen[46] verweigern, ansonsten muss dem Auftragnehmer ein entsprechendes Kündigungsrecht eingeräumt werden. Kann der Auftragnehmer aus seiner Sicht ohne die Hinzuziehung des Unterauftragnehmers seine vertragliche Leistung auf Grund der Verweigerung des Auftraggebers nicht erbringen, so muss er den Vertrag kündigen können.

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

[46] Hinweis: Wichtiger Grund ist ein Begriff aus dem deutschen Schuldrecht, eine Definition findet sich in § 314 BGB: Ein wichtiger Grund liegt vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zugemutet werden kann. Ein wichtiger Grund im Rahmen der Auftragsverarbeitung läge beispielsweise vor, wenn durch die Hinzuziehung des Unterauftragnehmers den aus der DS-GVO resultierenden Pflichten nicht mehr genügt werden kann.

müssen für die ordnungsgemäße Abwicklung des Auftrags zwingend Voraussetzung sein.

Unteraufträge sollten ausdrücklich festhalten, dass die Kontrollrechte des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten (§ 12 Ziff. 6), da der Auftraggeber sonst seiner gesetzlich vorgeschriebenen Verantwortung nicht nachkommen kann[47].

Ort der Leistungserbringung

Siehe Kommentierung § 6 auf Seite 46

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 2017-02-23]; 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 2017-02-23]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf
3) Bergt M. (2013) Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft. DuD: 796-801
4) Düsseldorfer Kreis. (2007) Internationaler Datenverkehr. [Online, zitiert am 2017-02-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/April07IntDatenverkehr.pdf?__blob=publicationFile
5) Düsseldorfer Kreis. (2010) Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen. [Online, zitiert am 2017-02-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile
6) Düsseldorfer Kreis. (2013) Datenübermittlung in Drittstaaten. [Online, zitiert am 2018-02-23]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/12092013DatenuebermittlungInDrittstaaten.pdf?__blob=publicationFile
7) Eckhardt J. (2013) Auftragsdatenverarbeitung - Gestaltungsmöglichkeiten und Fallstricke. DuD: 585-591
8) Erd R. (2011) Auftragsdatenverarbeitung in sicheren Drittstaaten. DuD: 275-278

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

9) Eul H, Eul P. (2011) Datenschutz International: Ein Praxisleitfaden für die Übermittlung von Kunden-, Mitarbeiter- und Lieferantendaten. 1. Auflage. Datakontext Verlag
10) Hoeren T. (2010) Das neue BDSG und die Auftragsdatenverarbeitung. DuD: 688-691
11) Kremer S. (2014) Leistungsketten in der Auftragsdatenverarbeitung - Anforderungen an die Einbeziehung von (Unter-)Unterauftragnehmern nach dem BDSG. ITRB: 60-66
12) Lensdorf L. (2010) Auftragsverarbeitung in der EU/EWR und UnterAuftragsverarbeitung in Drittländern - Besonderheiten der neuen EU-Standardvertragsklauseln. CR: 735-741
13) Moos F. (2010) Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010 - Die wesentlichen Neuerungen und Kritikpunkte im Überblick. CR: 281-286
14) Müthlein T. (2016) ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 74-87
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) Schmitz B, von Dall'Armi J. (2016) Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? - Wie Daten künftig von Dienstleistern verarbeitet werden müssen. ZD: 427432
18) 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
19) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand
20) Voigt P. (2012) Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland? ZD: 546-550
21) Weber M, Voigt P. (2011) Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. ZD: 74-78

§ 13 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

Kommentierung § 13

Um zu verhindern, dass der Auftragnehmer Daten des Auftraggebers nicht an den Auftraggeber herausgibt, verzichtet der Auftragnehmer durch diese vertragliche Vereinbarung auf die Geltendmachung jeglicher Zurückbehaltungsrechte an den vertragsgegenständlichen Daten – wie etwa gemäß §§ 273, 320 BGB, § 369 HGB.

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
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

§ 14 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

a. er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

Kommentierung § 14

Art. 82 DS-GVO regelt die datenschutzrechtlichen Aspekte einer Haftung und weist Auftraggeber sowie Auftragnehmer entsprechende Verantwortlichkeiten gegenüber einer betroffenen Person zu. Diese Verantwortlichkeiten sind vertraglich nicht abdingbar.

Der Auftragnehmer muss für alle wichtigen Pflichtverletzungen und Leistungsstörungen aufkommen und kann die Haftung nicht ausschließen.

Vom haftungsrechtlichen Anspruch unabhängig sind vertraglich vereinbarte Strafen. Eine Vertragsstrafe kann bis zur Grenze der Sittenwidrigkeit gemäß § 138 BGB beziffert werden[48]. 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.

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
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

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

§ 15 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung 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 Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 16 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.

(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.

1 # § 17 Rechtswahl, Gerichtsstand

2 (1) Es gilt deutsches Recht.

3 (2) Gerichtsstand ist der Sitz des Auftraggebers.

4

Kommentierung § 17

Rechtswahl

Nach Art. 3 Abs. 1 S. 1 Rom I-VO kann zwischen Auftraggeber und Auftragnehmer das anwendbare Recht grundsätzlich durch Rechtswahlklauseln festgelegt werden. Dabei muss die Rechtswahl ausdrücklich erfolgen oder sich eindeutig aus den Bestimmungen des Vertrags oder aus den Umständen des Einzelfalls ergeben. Umstritten ist dabei, ob Rechtswahlklauseln auch im Datenschutzrecht zulässig sind oder ob es sich bei diesen Regelungen um Eingriffsnormen i. S. v. Art. 9 Abs. 1 Rom I-VO handelt.

Ergibt sich der räumliche Anwendungsbereich des mitgliedstaatlichen Rechts aus den jeweiligen Öffnungsklauseln, so sind diese als speziellere Kollisionsnormen einer Rechtswahl der Parteien entzogen[49]. Insbesondere darf das Schutzniveau der DS-GVO nicht unterlaufen werden. Insofern sind Auftraggeber (Verantwortlicher) und Auftragnehmer (Auftragsverarbeiter) hinsichtlich der Vertragswahl eingeschränkt, i. d. R. wird als Rechtswahl nur das Recht des Mitgliedstaats wählbar sein, welches für den im Sinne der DS-GVO Verantwortlichen (= Auftraggeber) gilt.

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
3) Petri T. (2014) §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft
4) Sailer C. (2008) Rechtsnachfolge in Gerichtsstandsvereinbarung. JuBl (130): 389-392
5) Sommer I. (2011) §80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. in Krahmer (Hrsg.) Sozialdatenschutz nach SGB I und X. 3. Auflage. Luchterhand

[49] Laue P. (2016) Öffnungsklauseln in der DS-GVO – Öffnung wohin? Geltungsbereich einzelstaatlicher (Sonder-)Regelungen. ZD: 463-647

Anlage(n)

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen.

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

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Kommentierung Anlage 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.

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

Das Gliederungsschema gemäß der Anlage zu § 9 S. 1 BDSG wird vorerst weiterhin zur Verwendung vorgeschlagen, da es einerseits derzeit noch weit verbreitet ist und andererseits die DS-GVO mit ihren wesentlich abstrakteren Grundprinzipien/Gewährleistungszielen kein ähnlich operationales Schema anbietet.

1) Zutrittskontrolle

☐ Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil ...
☐ Es existieren keine Maßnahmen zur Zutrittskontrolle, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ 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, weil ...
☐ Es existieren folgende Maßnahmen zur Trennungskontrolle:
1) …
2) …
3) …

Kommentierung Anlage 2

Grundsätzlich muss jede Verarbeitung - und damit auch die Auftragsverarbeitung - geeignete technische und organisatorische Maßnahmen zum Schutz aufweisen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (Art. 32 Abs. 1 DS-GVO). Damit verbunden ist die Anforderung, dass die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen dargestellt und bewertet werden müssen. Erfolgt eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten“, was im Bereich der Gesundheitsversorgung ja nahezu immer zutrifft, muss laut Art. 35 Abs. 7 lit. c DS-GVO in der Datenschutz-Folgenabschätzung „eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen“ integriert sein, wobei Art. 25 Abs. 1 DS-GVO referenziert wird., d. h. Risiken „für die Rechte und Freiheiten natürlicher Personen“ müssen betrachtet werden. Hier sind also insbesondere die Risiken für die betroffene Person zu betrachten, die IT-Risiken für die verarbeitende Organisation sind hiervon nur sekundär berührt.

Aus dieser Risikofolgenabschätzung müssen Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen abgeleitet werden und genau diese Maßnahmen müssen hier aufgeführt werden. Es geht daher nicht mehr darum, die Liste aus dem Anhang zu § 9 BDSG abzuarbeiten bzw. abzuhaken, sondern es müssen genau die die Risiken verhindernden bzw. die die Risiken minimierenden Maßnahmen dargestellt werden.

Hierzu gehört natürlich auch, dass der Auftraggeber dem Aufragnehmer ggf. spezifische Risiken benennt, die dieser in seiner bzgl. bei ihm stattfindenden Auftragsverarbeitung betreffenden Risikofolgenabschätzung betrachtet und daraus die entsprechenden zu benennenden Maßnahmen ableitet.

Die technisch-organisatorischen Maßnehmen müssen sich dabei natürlich nicht von den bisherigen Maßnahmen, die entsprechend dem Anhang zu § 9 BDSG resultierenden Anforderungen getroffen wurden, unterscheiden. Jedoch müssen künftig natürlich nur die Maßnahmen benannt werden, die auch ein Risiko adressieren. Im AV-Vertrag bzw. dessen Anhang gehören allerdings nur die Maßnahmen hinein, nicht die vollständige Risikobetrachtung. Diese muss im Rahmen der aus Art. 5 DS-GVO resultierenden Nachweispflicht vorhanden sein und ggf. den zur Prüfung berechtigten Personen vorgelegt werden.

Es bietet sich an, die Maßnahmen auch künftig gruppiert darzustellen. Hierzu kann man sich der groben Maßnahmenstrukturierung aus dem Anhang zu § 9 BDSG bedienen. Ebenso ist eine Gliederung gemäß den in Art. 32 DS-GVO enthaltenen Anforderungen möglich. Eine entsprechende Gliederung könnte wie folgt aussehen:

- Verfahren zur Beurteilung des angemessenen Schutzniveaus unter Berücksichtigung einer Risikobetrachtung
- Verfahren, die Pseudonymisierung und Verschlüsselung nutzen
- Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
- Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung dienen

– Verfahren zur Gewährleistung, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Für die Maßnahmenkataloge der IT-Grundschutz-Kataloge des BSI gibt es Mapping-Tabelle zu den Anforderungen aus dem Anhang zu § 9 BDSG[50], desgleichen existiert eine Zuordnungstabelle bzgl. IT-Grundschutz und ISO 27001/ISO 27002[51]. Somit fällt auch eine Zuordnung von im Rahmen einer ISO 27001-Zertifizierung ergriffenen Maßnahmen zu den Kategorien des BDSG relativ leicht, so dass in Deutschland voraussichtlich diese Gruppierung noch einige Zeit erhalten bleiben wird.

1) Zutrittskontrolle

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

- Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte
- (Kontrollierte) Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung Alarmanlage, Video- / Fernsehmonitor

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

[50] BSI: „Maßnahmen und Datenschutz-Kontrollziele“, Stand 22.08.2007. [Online, zitiert am 2017-03-11]; Verfügbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile

[51] BSI: Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz. [Online, zitiert am 2017-03-11]; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile

- 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 TOMs 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 Auftragsverarbeitung 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

Beispiel für eine Vertraulichkeitserklärung zur Verpflichtung des eingesetzten Personals

gemäß Art. 28 Abs. 3 S. 2 lit. b der „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung, DS-GVO), auf das Fernmeldegeheimnis gemäß § 88 Telekommunikationsgesetz (TKG) und auf Wahrung von Geschäftsgeheimnissen.

_____

(Name der verantwortlichen Stelle)

_____ _____

(Name des Mitarbeiters) (Geburtsdatum)

1. Verpflichtung auf das Datengeheimnis nach Art. 28 Abs. 3 S. 2 lit. b DS-GVO[52]

Aufgrund von Art. 28 Abs. 3 S. 2 lit. b DS-GVO ist mir untersagt, personenbezogene Daten, die mir dienstlich bekannt werden, unbefugt zu verarbeiten. Dies gilt sowohl für die dienstliche Tätigkeit innerhalb wie auch außerhalb (z.B. bei Kunden und Interessenten) des Unternehmens/der Behörde.

Die Pflicht zur Wahrung des Datengeheimnisses bleibt auch im Falle einer Versetzung oder nach Beendigung des Arbeits-/Dienstverhältnisses bestehen, sofern keine Erlaubnistatbestände entsprechend Art. 6 bzw. - im Falle des Vorliegens besonderer Kategorien personenbezogener Daten - Art. 9 DS-GVO eine Verarbeitung erlauben.

2. Verpflichtung auf das Fernmeldegeheimnis

Aufgrund von § 88 TKG bin ich zur Wahrung des Fernmeldegeheimnisses verpflichtet, soweit ich im Rahmen meiner Tätigkeit bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirke.

3. Verpflichtung auf Wahrung von Geschäftsgeheimnissen

Über Angelegenheiten des Unternehmens, die beispielsweise Einzelheiten ihrer Organisation und ihrer Einrichtung betreffen, sowie über Geschäftsvorgänge und Zahlen des internen Rechnungswesens, ist – auch nach Beendigung des Arbeitsverhältnisses – von mir Verschwiegenheit zu wahren, sofern sie nicht allgemein öffentlich bekannt geworden sind. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen ich dienstlich befasst bin. Auf die gesetzlichen Bestimmungen über unlauteren Wettbewerb wurde ich besonders hingewiesen.

Alle, die dienstliche Tätigkeiten betreffenden Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen dienstlicher oder geschäftlicher Vorgänge, die mir überlassen oder von mir angefertigt werden, sind vor Einsichtnahme Unbefugter zu schützen.

[52] Bitte aktuelle Entwicklungen und ggf. Muster beobachten

Von diesen Verpflichtungen habe ich Kenntnis genommen. Ich bin mir bewusst, dass ich mich bei Verletzungen des Datengeheimnisses, des Fernmeldegeheimnisses oder von Geschäftsgeheimnissen strafbar machen kann, insbesondere nach Art. 84 DS-GVO i. V. m. dem deutschen Umsetzungsgesetz[53], § 206 Strafgesetzbuch (StGB) und nach § 17 Gesetz gegen den unlauteren Wettbewerb (UWG). Das Merkblatt zur Verpflichtungserklärung mit den Abschriften der genannten Vorschriften habe ich erhalten.

_____

Ort, Datum

_____ _____

(Unterschrift Verpflichteter) (Unterschrift Verpflichtender)

[53] Hier bitte nach Verkündung die entsprechenden Bestimmungen des neuen BDSG abbilden

Kommentierung Anlage 3

In den Zeilen 12 bis 23 erfolgt die Verpflichtung auf das Datengeheimnis, welche für Auftragsverarbeitung europarechtlich durch die DS-GVO vorgeschrieben ist.

In Zeilen 24 bis 26 erfolgt die Verpflichtung auf das Fernmeldegeheimnis entsprechend § 88 Telekommunikationsgesetz (TKG). Dieser Passus ist natürlich nur zu nutzen, wenn unter die Regelungen des TKG fallende Daten verarbeitet werden.

In den Zeilen 27 bis 38 wird eine Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen vorgenommen.

In den Zeilen 44 und 45 wird dargelegt, dass der Verpflichtete die gesetzlichen Tatbestände ausgehändigt bekam. Hier besteht ggf. Anpassungsbedarf.