Umgang mit Altverträgen bzgl. Auftragsverarbeitung („ADV-Verträge“)

Eine Zusammenarbeit von

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

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz

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 1.0

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
Jens Schwanke	Kairos 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. Diese Ausarbeitung ist 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 für diese Situation 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

Zusammenfassung

Die europäische Datenschutz-Grundverordnung (DS-GVO) regelt abschließend die Auftragsverarbeitung (AV), nationale Gesetzgeber können lediglich die Erlaubnistatbestände für eine Auftragsverarbeitung festlegen, wobei sie auch hierbei an die Rahmenbedingungen der DS-GVO gebunden sind. Damit existieren in Europa einheitliche datenschutzrechtliche Bedingungen zur Auftragsverarbeitung, unabhängig davon ob es sich hierbei um eine Auftragsverarbeitung im Rahmen einer medizinischen Forschung, der Patientenversorgung oder im Umfeld von „public health" handelt.

Schutzziel ist hierbei nicht der Ort der Verarbeitung, sondern der Schutz der personenbezogenen Daten. Folgerichtig ist die Auftragsverarbeitung entsprechend der DS-GVO im Gegensatz zu den Vorgaben des BDSG auch nicht örtlich begrenzt; eine Auftragsverarbeitung kann weltweit, d.h. auch außerhalb der EU in einem Drittland, erfolgen, sofern der von der DS-GVO vorgeschriebene Schutz der Daten gewährleistet ist.

Die DS-GVO verlangt ausdrücklich einen Vertrag oder „ein anderes Rechtsinstrument" für eine Auftragsvergabe durch einen Aufragnehmer, § 11 BDSG verlangte hier „nur" einen schriftlichen „Auftrag". Allerdings wurden in Deutschland überwiegend ADV-Verträge geschlossen, sodass diese Anforderung für deutsche Auftraggeber (in der DS-GVO „Verantwortliche" genannt) keine Herausforderung darstellen sollte. Aber anders als im BDSG ist der Auftragsverarbeiter nunmehr neben dem Verantwortlichen eigenständiger Normadressat und hat eigenständige Pflichten auferlegt bekommen, inklusive eigener Bußgeldtatbestände.

Die aus dem deutschen Recht bekannte Privilegierung der Auftragsverarbeitung wurde beibehalten, sodass auch unter dem europäischen Recht eine Auftragsverarbeitung keinen eigenen Erlaubnistatbestand benötigt; der Auftragsverarbeiter zählt datenschutzrechtlich quasi zum Verantwortlichen (im Rahmen des BDSG als „verantwortliche Stelle" bezeichnet).

Wartung und Fernwartung sind in der DS-GVO im Gegensatz zum BDSG nicht speziell geregelt. Sofern im Rahmen einer Wartung/Fernwartung ein Zugriff auf personenbezogene Daten nicht sicher vermieden werden kann, wird man aber auch nach der DS-GVO einen Vertrag zur Auftragsverarbeitung abschließen müssen.

1 Allgemeines

Die am 24. Mai 2016 in Kraft getretene europäische Datenschutz-Grundverordnung (DS-GVO), die ab dem 25. Mai 2018 in Europa unmittelbar geltendes Recht sein wird, übernimmt im Kern die aus der Richtlinie 95/46/EG („Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr") bekannten datenschutzrechtlichen Grundprinzipien wie die der „Datenvermeidung und Datensparsamkeit", der „Zweckbindung", des „Verbots mit Erlaubnisvorbehalts" und der „Transparenz". Oftmals wird daher gesagt, dass sich im Prinzip nichts ändert, was in gewisser Hinsicht sicherlich stimmt. Schaut man sich die Regelungen im Einzelnen an, findet man hingegen eine Vielzahl von Neuerungen und Änderungen zum bestehenden geltenden Recht. In manchen Details gibt es sogar großen Anpassungsbedarf. Dies gilt auch für die Auftragsverarbeitung. Im Folgenden sollen in aller Kürze die geänderten oder auch neuen Aspekte vorgestellt werden.

2 Pflichten für den Auftragsverarbeiter

Anders als im BDSG heißt der Auftragnehmer in der DS-GVO „Auftragsverarbeiter“. Nach der DS-GVO ist der Auftragsverarbeiter nunmehr neben dem Verantwortlichen eigenständiger Normadressat. Ihm stehen ferner eigene, aus der DS-GVO resultierende Rechte und Pflichten zu, deren Nichteinhaltung bußgeldbewehrt ist. Diese Pflichten sind im Nachfolgenden tabellarisch aufgeführt.

	DS-GVO	Inhalt der Regelung
Vertreterregelung	Art. 27 Abs. 1, 3	Auftragsverarbeiter außerhalb der EU müssen schriftlich einen Vertreter in der Union bestimmen, der in einem der Mitgliedstaaten niedergelassen sein muss, welcher insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Einhaltung der Vorgaben der DS-GVO als Anlaufstelle dient.
Unterauftrags-verarbeiter	Art. 28 Abs. 2	Der Auftragsverarbeiter darf ohne schriftliche Genehmigung des Verantwortlichen keinen Unterauftragsverarbeiter beauftragen. Hinweis: Eine elektronische Form der Genehmigung sieht Art. 28 Abs.2 DS-GVO nicht vor.
Dokumentation der Weisung und Ausführung	Art. 28 Abs. 3 lit a	Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten. Dies beinhaltet auch die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. **Hinweis:** Dies bedeutet, dass auch im Rahmen der Wartung/ Fernwartung eines IT-Systems diese Wartung/Fernwartung nur auf eine dokumentierte Weisung des Verantwortlichen hin erfolgen darf; der Auftragsverarbeiter hat hier keinen Ermessungsspielraum.
Verpflichtung zur Vertraulichkeit	Art. 28 Abs. 3 lit. b	Der Aufragnehmer muss gewährleisten, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
Geeignete technische und organisatorische Maßnahmen	Art. 28 Abs. 3 lit. c i. V. m. Art. 32	Der Auftragsverarbeiter muss erforderliche technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO umsetzen.
Betroffenenrechte	Art. 28 Abs. 3 lit. e	Der Auftragsverarbeiter muss mit geeigneten technischen und organisatorischen Maßnahmen den Verantwortlichen in der Umsetzung der Rechte von betroffenen Personen unterstützen.
Unterstützung des	Art. 28 Abs. 3	Der Auftragsverarbeiter muss, soweit ihm dies nach der Art der Verarbeitung und der ihm zur Verfügung stehenden

	DS-GVO	Inhalt der Regelung
Verantwortlichen	lit. f	Informationen möglich ist, den Verantwortlichen bei der Einhaltung der Anforderungen von – Art. 32 (Sicherheit der Verarbeitung) – Art. 33 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) – Art. 34 (Meldung von Verletzungen des Schutzes personenbezogener Daten an den Betroffenen) – Art. 35 (Datenschutz-Folgenabschätzung) – Art. 36 (Vorherige Konsultation der Aufsichtsbehörde) unterstützen.
Rückgabe der Daten	Art. 28 Abs. 3 lit. g	Nach Abschluss der Verarbeitung muss der Auftragsverarbeiter die personenbezogenen Daten löschen oder zurückgeben, sofern für den Auftragsverarbeiter keine rechtliche Verpflichtung zur Aufbewahrung der personenbezogenen Daten besteht.
Dokumentation	Art. 28 Abs. 3 lit. h	Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung stellen.
Kontrollen	Art. 28 Abs. 3 lit. h	Der Auftragsverarbeiter muss Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und unterstützen.
Mitteilungspflicht bei unzulässigen Weisungen	Art. 28 Abs. 3 Satz 3	Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich informieren, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.
Unterauftrags-verarbeiter	Art. 28 Abs. 4	Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter, so muss er dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegen, die der Auftragsverarbeiter mit dem Verantwortlichen vereinbarte. Außerdem haftet der Auftragsverarbeiter für Pflichtverletzungen des Unterauftragsverarbeiters.
Weisungsbefugnis	Art. 29	Der Auftragsverarbeiter darf personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten, außer dass er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist. **Hinweis:** Ist dies der Fall, so muss der Auftragsverarbeiter vor Beginn der Verarbeitung den Verantwortlichen über diese rechtlichen Anforderungen zur Verarbeitung seiner Daten

	DS-GVO	Inhalt der Regelung
		informieren (Art. 28 Abs. 3 lit. a), sofern dieses Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
Verzeichnis von Verarbeitungs-tätigkeiten	Art. 30 Abs. 2 i. V. m. Art. 30 Abs. 3	Der Auftragsverarbeiter führt (soweit keine Ausnahmetatbestände vorliegen) ein schriftliches (beinhaltet auch die Möglichkeit der Nutzung eines elektronischen Formates) Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.
Zusammenarbeit mit Aufsichtsbehörden	Art. 30 Abs. 4	Der Auftragsverarbeiter stellt das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.
Zusammenarbeit mit Aufsichtsbehörden	Art. 31	Der Auftragsverarbeiter arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
Weisungsbefugnis	Art. 32 Abs. 4	Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen die personenbezogenen Daten nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind rechtlich zur Verarbeitung verpflichtet.
Mitteilungspflicht bei Pannen	Art. 33 Abs. 2	Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich über eine Verletzung des Schutzes personenbezogener Daten informieren.
Datenschutz-beauftragter	Art. 37 Abs. 1, Abs. 4 S. 1, 2. HS	Der Auftragsverarbeiter muss einen Datenschutzbeauftragten bestellen, wenn dies durch die DS-GVO oder nach einem anderen Recht der Union oder der Mitgliedstaaten vorgeschrieben ist.
Datenschutz-beauftragter	Art. 38 Abs. 1	Der Auftragsverarbeiter muss gewährleisten, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden ist.
Datenschutz-beauftragter	Art. 38 Abs. 2	Der Auftragsverarbeiter stellt dem Datenschutzbeauftragten alle erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen als auch die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung.
Datenschutz-beauftragter	Art. 38 Abs. 3	Der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben weisungsfrei arbeiten kann. Der Datenschutzbeauftragte darf wegen seiner Aufgabenerfüllung nicht abberufen oder benachteiligt werden.

	DS-GVO	Inhalt der Regelung
Datenschutz-beauftragter	Art. 38 Abs. 6	Nimmt der Datenschutzbeauftragte noch andere Aufgaben und Pflichten wahr, stellt der Auftragsverarbeiter sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
Drittländer	Artt. 44-50	Eine Verarbeitung in Drittländern ist nur unter Einhaltung der in den Artt. 44-50 DS-GVO beschriebenen Anforderungen statthaft.
Zusammenarbeit mit Aufsichtsbehörden	Art. 60 Abs. 10	Nach der Unterrichtung durch eine federführende Aufsichtsbehörde muss der Auftragsverarbeiter die erforderlichen Maßnahmen treffen, um die Entscheidung der Aufsichtsbehörde umzusetzen. Diese getroffenen Maßnahmen muss der Auftragsverarbeiter der federführenden Aufsichtsbehörde mitteilen.
Haftung	Art. 82 Abs. 2	Der Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen gehandelt hat oder gegen diese Anweisungen gehandelt hat.
Haftung	Art. 82 Abs. 4	Jeder Verantwortliche oder jeder Auftragsverarbeiter haftet für den gesamten Schaden, damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist.

3 Vertragsrelevante Regelungen

3.1 Formvorgaben

Art. 28 Abs. 3 DS-GVO verlangt ausdrücklich einen Vertrag oder „ein anderes Rechtsinstrument“. Gemäß Art. 28 Abs. 9 DS-GVO muss der Vertrag schriftlich abgefasst werden, wobei eine entsprechende Schriftform auch ein elektronisches Format aufweisen darf. Vgl. hinsichtlich näherer Ausführungen die diesbezügliche Darstellung unter 3.2 zu Art. 28 Abs. 9.

Neben einem individuellen Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter können gemäß Art. 28 Abs. 6 DS-GVO künftig Standardvertragsklauseln verwendet werden, die entweder von der EU-Kommission oder nach dem neu eingeführten Kohärenzverfahren festgelegt werden (Art. 28 Abs. 7, 8 DS-GVO).

3.2 Beibehaltene vertragsrelevante Regelungen

Darstellung der im BDSG bereits enthaltenen Regelungen, die sich praktisch unverändert in der DS-GVO wiederfinden.

	BDSG	DS-GVO	Inhalt der Regelung
Gegenstand/ Dauer	§ 11 Abs. 2 Ziff. 1	Art. 28 Abs. 3 S. 1	Festzulegen sind: Gegenstand und Dauer der Verarbeitung
Art/Zweck	§ 11 Abs. 2 Ziff. 2	Art. 28 Abs. 3 S. 1	Festzulegen sind: Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen
Löschung	§ 11 Abs. 2 Ziff. 10	Art. 28 Abs. 3 lit. g	Der Auftragsverarbeiter löscht oder gibt alle personenbezogenen Daten an den Verantwortlichen entsprechend dessen Entscheidung zurück.
Hinweispflicht	§ 11 Abs. 3 S. 2	Art. 28 Abs. 3 S. 3	Es besteht eine Hinweispflicht, wenn der Auftragsverarbeiter eine Weisung des Verantwortlichen für datenschutzrechtlich rechtswidrig hält.

3.3 Geänderte vertragliche Regelungen

Die nachfolgenden Regelungen sind bisher grundsätzlich in § 11 BDSG enthalten. In der DS-GVO sind sie etwas abgeändert oder genauer spezifiziert vorhanden.

	DS-GVO	Inhalt der Regelung
Begriffsdefinition Auftragsverarbeiter	Art. 4 Ziff. 8	Während im BDSG der Begriff des „Auftragsverarbeiters“ nicht explizit enthalten und definiert ist, definiert die DS-GVO, was unter diesem Begriff zu verstehen ist. Dabei bleibt die DS-GVO bei der Begriffsbestimmung, wie sie aus der RL 95/46/EG bekannt ist, sodass bisherige Ausführungen der Aufsichtsbehörden[1] zur Interpretation herangezogen werden können.
Drittland	Art. 4 Ziff. 10	Im Unterschied zu der entsprechenden Regelung im BDSG ist ein Auftragsverarbeiter mit einem Sitz im Drittland nicht automatisch „Dritter“. Ob die Definition des „Dritten“ auf eine datenverarbeitende Stelle zutrifft, hängt ausschließlich von der Befugnis ab, ob die Daten unter der Verantwortung eines Verantwortlichen als Auftragsverarbeiter verarbeitet werden

[1] z. B. Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169 vom 16.2.2010, S. 32. Online, zitiert am 2016-09-25; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

	DS-GVO	Inhalt der Regelung
		dürfen, nicht vom Erbringungsort.
Verpflichtung zur Vertraulichkeit	Art. 28 Abs. 3 lit. b	Der Auftragsverarbeiter muss gewährleisten, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
Geeignete technische und organisatorische Maßnahmen	Art. 28 Abs. 3 lit. c	Der Auftragsverarbeiter muss erforderliche technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO umsetzen.
Unterauftrags-verarbeiter	Art. 28 Abs. 3 lit. d	Der Auftragnehmer darf keine weiteren Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Auftraggebers in Anspruch nehmen. Im Fall einer allgemeinen Genehmigung ist über die beabsichtigte Änderung der Hinzuziehung zu informieren, um dem Auftraggeber die Möglichkeit des Einspruchs einzuräumen.
Rechte betroffener Personen	Art. 28 Abs. 3 lit. e	Der Auftragsverarbeiter muss mit geeigneten technischen und organisatorischen Maßnahmen den Verantwortlichen bei der Umsetzung der Rechte von betroffenen Personen unterstützen.
Unterstützung des Verantwortlichen	Art. 28 Abs. 3 lit. f	Der Auftragsverarbeiter muss, soweit ihm dies nach der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen möglich ist, den Verantwortlichen bei der Einhaltung der Anforderungen von – Art. 32 (Sicherheit der Verarbeitung) – Art. 33 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) – Art. 34 (Meldung von Verletzungen des Schutzes personenbezogener Daten an den Betroffenen) – Art. 35 (Datenschutz-Folgenabschätzung) – Art. 36 (Vorherige Konsultation der Aufsichtsbehörde) unterstützen
Form	Art. 28. Abs. 3 S.1, S. 2 Art. 28 Abs. 9	Die DS-GVO verlangt ausdrücklich einen schriftlichen Vertrag (BDSG nur einen „schriftlich zu erteilenden Auftrag“), wobei diese Anforderung auch ein elektronisches Format zulässt. ErwGr. 32 gibt Hinweise, was der europäische Verordnungsgeber unter einer „elektronischen Form“ in Bezug auf die Einwilligung versteht. Diese können analog zur Interpretation im Rahmen der Vertragsgestaltung bei der Auftragsverarbeitung hinzugezogen werden.

	DS-GVO	Inhalt der Regelung
Rechenschaftspflicht		Art. 5 Abs. 2 DS-GVO erhebt eine „Rechenschaftspflicht“ bezüglich der Anforderungen von Art. 5 Abs. 1 DS-GVO. **Hinweis:** Neben der Nachweis- und Rechenschaftspflicht gegenüber dem Betroffenen muss diese Dokumentation letztlich auch einer aufsichtsrechtlichen/gerichtlichen Überprüfung standhalten. Daher bietet es sich an, einen Vertrag entsprechend der deutschen Vorgaben gemäß §§ 126, 126a BGB abzuschließen.
Dokumentation	Art. 30 Abs. 4	Der Auftragsverarbeiter stellt das von ihm erstellte „Verzeichnis von Verarbeitungstätigkeiten“ auf Anfrage der Aufsichtsbehörde zur Verfügung. D. h. der Auftragsverarbeiter muss direkt mit der Aufsichtsbehörde zusammenarbeiten, unabhängig vom Verantwortlichen. **Hinweis:** Daher sollte vertraglich vereinbart werden, dass der Auftragsverarbeiter den Verantwortlichen von diesen Anfragen der Aufsichtsbehörde informiert.
Technische und organisatorische Maßnahmen	Art. 32 Abs. 1	Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung zu gewährleisten. Dies muss unter Berücksichtigung - des Stands der Technik, - der Implementierungskosten und - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie - der unterschiedlichen Eintrittswahrscheinlichkeit und - der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen erfolgen. Die getroffenen Maßnahmen müssen der Aufzählung in Art. 32 Abs. 1 lit. a-d genügen.
Information bei Verletzungen	Art. 33 Abs. 2	Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich über eine Verletzung des Schutzes personenbezogener Daten informieren.
Bußgeld	Art. 83 Abs. 4 lit. a	Im Unterschied zum BDSG ist nicht ein bestimmtes Verhalten oder Unterlassen bußgeldbewehrt, sondern jeder Verstoß gegen die aufgeführten Artikel der DS-GVO bzw. den daraus resultierenden Pflichten für Verantwortliche und Auftraggeber. Zudem enthält der Wortlaut eine „muss“-Vorgabe, so dass die Aufsichtsbehörde jeden Verstoß ahnden muss.

3.4 Neue vertragliche Regelungen

	DS-GVO	Inhalt der Regelung
Vertreter	Art. 27 Abs. 1	Verantwortliche oder Auftragsverarbeiter müssen schriftlich einen Vertreter in der Union benennen, wenn ein Drittstaatenbezug gemäß Art. 3 Abs. 2 vorliegt. Der Vertreter kann sowohl eine natürliche als auch eine juristische Person sein (Art. 4 Nr. 17).
Vertreter	Art. 27 Abs. 2	Art. 27 Abs. 2 schränkt die aus Art. 27 Abs. 1 resultierende Pflicht zur Benennung eines Vertreters in der Union ein. Die Pflicht gilt prinzipiell nicht für Behörden oder öffentliche Stellen (Art. 27 Abs. 2 lit. b). Diese Ausnahmeregelung muss immer individuell geprüft werden, da Art. 27 Abs. 2 lit a fordert, „unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung“ das „Risiko für die Rechte und Freiheiten natürlicher Personen“ einzuschätzen. **Hinweis:** Nur wenn diese Risikoabwägung ergibt, dass keine besonderen Risiken mit der Verarbeitung verbunden sind, kommen die angegebenen Ausnahmetatbestände zur Wirkung[2].
Vertreter	Art. 27 Abs. 3	Der in Art. 27 Abs. 1 geforderte Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren Daten verarbeitet werden, leben. **Hinweis:** Die Formulierung „in einem der Mitgliedsstaaten“ lässt darauf schließen, dass die Benennung nur eines Vertreters ausreichend ist[3].
Vertreter	Art. 27 Abs. 4	Der Vertreter muss durch den Verantwortlichen oder den Auftragsverarbeiter beauftragt werden, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung als Anlaufstelle zu dienen.
Haftung	Art. 27 Abs. 5	Die Verantwortung und Haftung des Verantwortlichen oder des Auftragsverarbeiters ist unabhängig von der Bestellung eines Vertreters, d.h. ein Betroffener hat immer die

[2] Plath KU (2016) Art. 27 DS-GVO, Rn. 4 in Plath (Hrsg.) BDSG/DSGVO Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Verlag. ISBN 978-3-504-56074-4

[3] Plath KU (2016) Art. 27 DS-GVO, Rn. 5 in Plath (Hrsg.) BDSG/DSGVO Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Verlag. ISBN 978-3-504-56074-4

	DS-GVO	Inhalt der Regelung
		Möglichkeit, rechtliche Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst einzuleiten.
Unterauftrags-verarbeiter	Art. 28 Abs. 2 Art. 28 Abs. 3 S. 2 lit. d	Der Auftragsverarbeiter darf ohne schriftliche Genehmigung des Verantwortlichen keinen Unterauftragsverarbeiter beauftragen. **Hinweis:** die DS-GVO fordert explizit die Schriftform (Unterschrift). Die Möglichkeit der elektronisch erteilten Genehmigung sieht Art. 28 Abs.2 DS-GVO nicht explizit vor[4].
Dokumentation	Art. 28 Abs. 3 lit. a	Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten. Dies beinhaltet auch die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. **Hinweis:** D. h. auch im Rahmen der Wartung/Fernwartung eines IT-Systems darf diese Wartung/Fernwartung nur auf dokumentierte Weisung des Verantwortlichen erfolgen; der Auftragsverarbeiter hat hier keinen Ermessungsspielraum.
Unterauftrags-verarbeiter	Art. 28 Abs. 4	Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter, so muss er diesem dieselben Datenschutzpflichten auferlegen, die der Auftragsverarbeiter mit dem Verantwortlichen vereinbarte. Außerdem haftet der Auftragsverarbeiter für Pflichtverletzungen des Unterauftragsverarbeiters. **Hinweis:** Ähnlich lautende Formulierungen waren bisher in vielen Musterverträgen nach § 11 BDSG enthalten, gesetzlich aber nicht verpflichtend gefordert.
Genehmigte Verhaltensregeln, Zertifizierungs-verfahren	Art. 28 Abs. 5	Die Einhaltung genehmigter Verhaltensregeln (Art. 40) oder eines genehmigten Zertifizierungsverfahrens (Art. 42) durch einen Auftragsverarbeiter kann ggfs. als Bestandteil des Nachweises geeigneter technischer und organisatorischer Maßnahmen für hinreichende Garantien im Sinne der Art. 28

[4] ErwGr. 32 gibt Hinweise, was der europäische Gesetzgeber unter einer „elektronischen Form“ in Bezug auf die Einwilligung versteht, und kann analog zur Interpretation zu den Anforderungen bei der Vertragsgestaltung durchaus hinzugezogen werden. Der europäische Verordnungsgeber verwendet die Formulierung „elektronisches Format“ innerhalb der Erwägungsgründe der DS-GVO i.d.R. im Zusammenhang mit Internetseiten (bspw. ErwGr. 58: „Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website“). ErwGr. 32 beschreibt als Beispiel für das elektronische Format „Dies könnte etwa durch Anklicken eines Kästchens [...]“. Gemäß ErwGr. 32, 58 genügt in der DS-GVO eine entsprechende Dokumentation hinsichtlich des elektronischen Formats. Damit entspricht die angesprochene europäische Anforderung nicht der deutschen Schriftform gemäß §§ 126, 126a BGB.

	DS-GVO	Inhalt der Regelung
		Abs. 1 und 4 angesehen werden.
Standardvertrags-klauseln	Art. 28 Abs. 6	Ein individueller Vertrag zwischen Verantwortlichem und Auftragsverarbeiter kann ganz oder teilweise auf den in Art. 28 Abs. 7, 8 genannten Standardvertragsklauseln beruhen.
Standardvertrags-klauseln	Art. 28 Abs. 7	Die Kommission kann Standardvertragsklauseln zur Regelung der in Art. 28 Abs. 3, 4 genannten Anforderungen festlegen.
Standardvertrags-klauseln	Art. 28 Abs. 8	Eine Aufsichtsbehörde kann Standardvertragsklauseln zur Regelung der in Art. 28 Abs. 3, 4 genannten Anforderungen festlegen.
Verantwortung	Art. 28 Abs. 10	Der Auftragsverarbeiter gilt selbst als Verantwortlicher, wenn er entgegen den Vorgaben von Art. 28 DS-GVO die Zwecke und Mittel der Verarbeitung selber bestimmt.
Weisungsbefugnis	Art. 29	Der Auftragsverarbeiter darf personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten, außer dass er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist. Ist dies der Fall, so muss der Auftragsverarbeiter vor Beginn der Verarbeitung den Verantwortlichen über diese rechtlichen Anforderungen zur Verarbeitung seiner Daten informieren (Art. 28 Abs. 3 lit. a), sofern dieses Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
Verzeichnis von Verarbeitungs-tätigkeiten	Art. 30 Abs. 2	Der Auftragsverarbeiter führt ein schriftliches (beinhaltet auch die Möglichkeit der Nutzung eines elektronischen Formates) Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.
Zusammenarbeit mit Aufsichts-behörde	Art. 31	Der Verantwortliche und der Auftragsverarbeiter sowie deren etwaige Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. **Hinweis:** Da hier eine vom Verantwortlichen unabhängige Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde existiert, sollte vertraglich eine Informationspflicht gegenüber dem Verantwortlichen vereinbart werden.
Anwendungs-bereich	Art. 44	Hier wird der Anwendungsbereich von Kap. V (Übermittlung personenbezogener Daten an Drittländer oder an

	DS-GVO	Inhalt der Regelung
		internationale Organisationen) dargestellt. **Hinweis:** Alle Übermittlungen von Daten, die in einem Drittland (oder einer internationalen Organisation) verarbeitet werden bzw. dort verarbeitet werden sollen, bedürfen einer besonderen Rechtfertigung. Natürlich müssen auch die anderen Anforderungen der DS-GVO eingehalten werden. ErwGr. 101 führt hierzu aus, dass insbesondere das Schutzniveau bei der Übermittlung personenbezogener Daten in ein Drittland erhalten bleibt.
Schadenersatz	Art. 82 Abs. 1	Jede Person (ggfs. muss die Person nicht selbst ein Betroffener sein), der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. **Hinweis:** Innerhalb der DS-GVO existiert keine Beschränkung eines Ersatzanspruches für immaterielle Schäden, wie das bisherige deutsche Recht (§ 8 Abs. 3 BDSG) es vorsieht. Gleichfalls fehlt eine Begrenzung auf „schwere Persönlichkeitsverletzungen“ (§ 8 Abs. 2 BDSG). Insoweit wurde der Haftungsanspruch eines Geschädigten gegenüber Verantwortlichen und Auftragsverarbeitern erweitert.
Haftung	Art. 82 Abs. 2	Generell haftet jeder Verantwortliche für einen Schaden, der durch eine Verarbeitung verursacht wurde, die nicht den Anforderungen der DS-GVO genügt. Der Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er - seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder - unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen gehandelt hat oder - gegen diese Anweisungen gehandelt hat.
Haftung	Art. 82 Abs. 3	Kann der Verantwortliche bzw. der Auftragsverarbeiter nachweisen, dass er für den Umstand, durch den der Schaden eintrat, in keinerlei Hinsicht verantwortlich ist, so wird er von der Haftung befreit. **Hinweis:** Rechtswidriger Zugriff auf Daten durch Dritte („Hackerangriff“) beinhaltet hierbei, dass der Verantwortliche

	DS-GVO	Inhalt der Regelung
		bzw. der Auftragsverarbeiter nachweisen kann, dass entsprechende Schutzmaßnahmen gemäß Art. 32 (insbesondere dem Stand der Technik genügende Maßnahmen) etabliert waren[5]. Die Nachweispflicht liegt beim Verantwortlichen bzw. Auftragsverarbeiter, nicht jedoch beim Betroffenen.
Haftung	Art. 82 Abs. 4	Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt, so haftet jeder von ihnen für den gesamtem Schaden (Verantwortlichkeit für den Schaden vorausgesetzt). **Hinweis:** Hier liegt eine gesamtschuldnerische Haftung (vgl. § 421 BGB) gegenüber dem Betroffenen vor, so dass der Betroffene seinen Schadenersatzanspruch jeder Partei gegenüber geltend machen kann.
Haftung	Art. 82 Abs. 5	Hat ein Verarbeiter entsprechend Art. 82 Abs. 4 vollständigen Schadenersatz für einen erlittenen Schaden geleistet, so regelt Art. 82 Abs. 5 den Ausgleich im Innenverhältnis zwischen den verarbeitenden Parteien, so dass jede am Schaden beteiligte Partei sich auf Anforderung entsprechend ihrem Anteil am Schaden auch am Schadenersatz beteiligen muss.

4 Vertragsunabhängige Regelungen

In diesem Abschnitt erfolgt eine Darstellung ggf. AV-relevanter Regelungen, die nicht notwendigerweise Bestandteil eines AV-Vertrages sind.

4.1 Geänderte Regelungen

	DS-GVO	Inhalt der Regelung
Definition Verantwortlicher	Art. 4 Ziff. 7	Die Definition des Verantwortlichen hat sich geändert: natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

[5] Becker T (2016) Art. 82 DS-GVO, Rn. 5 in Plath (Hrsg.) BDSG/DSGVO Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Verlag. ISBN 978-3-504-56074-4

	DS-GVO	Inhalt der Regelung
Gemeinsame Verantwortliche	Art. 26 Abs. 3	Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so agieren sie als „gemeinsam für die Verarbeitung Verantwortliche“. Ein Betroffener kann seine aus der DS-GVO resultierenden Rechte gegenüber jedem Einzelnen der Verantwortlichen geltend machen. **Hinweis:** Auch gemeinsam für die Verarbeitung Verantwortliche können einen oder mehrere Auftragsverarbeiter einsetzen.
Definition Verarbeitung	Art. 28 Abs. 1 S. 1, 1. HS	Der Begriff der „Verarbeitung“ aus der DS-GVO beschränkt im Gegensatz zum BDSG eine Auftragsverarbeitung nicht auf eine rein technische Unterstützung.
Verantwortung	Art. 28 Abs. 1 S. 1, 2. HS	Die Regelung ähnelt den Vorgaben des § 11 BDSG, jedoch ist neben dem Verantwortlichen der Auftragsverarbeiter gleichrangiger Normadressat. **Hinweis:** Die Verpflichtung zur Einhaltung der Regelungen der DS-GVO ist nun Aufgabe von beiden: Auftragsverarbeiter sowie Verantwortlicher. Beiden kann bei Nicht-Einhaltung der Regelungen ein Bußgeld drohen. Gegen beide kann ein Betroffener ggf. haftungsrechtliche Ansprüche geltend machen.
Datenschutz-beauftragter	Art. 37 Abs. 1, Art. 37 Abs. 4	Der Verantwortliche oder Auftragsverarbeiter muss einen Datenschutzbeauftragten bestellen, wenn dies durch die DS-GVO oder nach einem anderen Recht der Union oder der Mitgliedstaaten vorgeschrieben ist.
Haftung	Art. 83 Abs. 3	Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

4.2 Neue Regelungen

	DS-GVO	Inhalt der Regelung
Datenschutz-beauftragter	Art. 38 Abs. 1	Der Verantwortliche oder der Auftragsverarbeiter muss gewährleisten, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden ist.
Datenschutz-beauftragter	Art. 38 Abs. 2	Der Verantwortliche oder der Auftragsverarbeiter stellt dem Datenschutzbeauftragten alle für die Erfüllung seiner Aufgaben erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen als auch die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung.
Zusammenarbeit mit Aufsichts-behörde	Art. 60 Abs. 10	Nach der Unterrichtung durch eine federführende Aufsichtsbehörde müssen der Verantwortliche und der Auftragsverarbeiter die erforderlichen Maßnahmen ergreifen, um der Entscheidung der Aufsichtsbehörde zu genügen. Diese getroffenen Maßnahmen müssen der Verantwortliche und der Auftragsverarbeiter der federführenden Aufsichtsbehörde mitteilen.

5 Weggefallene Regelungen

Aus dem BDSG bekannte, in der DS-GVO jedoch nicht mehr vorkommende Regelungen:

	BDSG	Inhalt der Regelung
Unterscheidung öffentlich / nicht-öffentlich	§ 11 Abs. 2 S. 3	„Er *[Der Auftrag]* kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden“ **Hinweis:** Die DS-GVO unterscheidet nicht zwischen öffentlichen und nicht-öffentlichen Stellen. Dementsprechend enthält die DS-GVO auch keine Regelung, wer in einer öffentlichen Stelle eine Auftragsverarbeitung genehmigen darf.
Kontrollen	§ 11 Abs. 2 S. 4, 5	„Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.“ Die DS-GVO fordert eine entsprechend sorgfältige Auswahl des Auftragsverarbeiters. Sie beinhaltet aber keine explizite Notwendigkeit des „Überzeugenmüssens“ von den ordnungsgemäßen technischen und organisatorischen

	BDSG	Inhalt der Regelung
		Maßnahmen vor und während der Verarbeitung. Indirekt kann jedoch aus den Regelungen der DS-GVO eine entsprechende Prüfverpflichtung aus Art. 32 Abs. 1 lit. d abgeleitet werden.
Einschränkung des Geltungsumfangs des BDSG bzw. Unterscheidung öffentlich / nicht-öffentlich	§ 11 Abs. 4	„Für den Auftragnehmer gelten neben den §§ [...]“ Die DS-GVO enthält explizite Regelungen für den Auftragsverarbeiter, daneben implizit geltende Regelungen, die für jeden Verarbeiter von Daten gelten. Die in § 11 Abs. 4 BDSG enthaltenen Regelungen bzgl. Datengeheimnis, TOMs, Bußgeldern und Benennung eines Datenschutzbeauftragten finden sich in der DS-GVO verteilt auf verschiedene Artikel, ohne jedoch für öffentliche und nicht-öffentliche Stellen unterschiedliche Regelungen aufzuführen; für beide soll grundsätzlich gleiches Recht gelten.
Wartung als ADV	§ 11 Abs. 5	„Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.“ Entfällt, siehe Kapitel 6.2

6 Spezielle Fragestellungen

6.1 Privilegierung der Auftragsverarbeitung

Die Auftragsverarbeitung wird in Deutschland als „privilegierter“ Tatbestand betrachtet, da die Weitergabe von Daten von dem Verantwortlichen an den Auftragsverarbeiter keiner weiteren gesetzlichen Rechtfertigung bedarf. Dies wird aus der Tatsache gefolgert, dass diese Weitergabe keine Übermittlung im Sinne von § 3 Abs. 4 Ziff. 3 BDSG darstellt, da der Auftragsverarbeiter entsprechend § 3 Abs. 8 S. 3 BDSG kein Dritter im Sinne des Gesetzes ist.

Vereinzelt wird argumentiert, dass diese Privilegierung mit Wirksamwerden der DS-GVO entfällt[6]. Diese Auffassung überzeugt nicht und entspricht auch nicht der herrschenden Meinung[7,8,9,10,11]. Die

[6] Laue P, Nink J, Kremer S. (2016) Das neue Datenschutzrecht in der betrieblichen Praxis. § 5 Rn. 4. Nomos Verlagsgesellschaft. 1. Auflage. ISBN 978-3-8487-2377-5

[7] Schmitz B, Dall’Armi J. (2013) Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? ZD: 427-432

[8] Plath KU (2016) Art. 28 DS-GVO, Rn. 3 in Plath (Hrsg.) BDSG/DSGVO Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Verlag. ISBN 978-3-504-56074-4

[9] Albrecht JP, Jotzo F. (2016) Das neue Datenschutzrecht der EU. Teil 5 „Verantwortlichkeiten und Pflichten“, Rn. 22. Nomos Verlag. ISBN 978-3-8487-2804-6

[10] Martini M. (2016) Art. 28 DS-GVO, Rn. 18 in Paal/Paul (Hrsg.) Datenschutz-Grundverordnung. C.H.Beck Verlag. ISBN 978-3-406-69570-4

Komplexität dieser Fragestellung zeigt Hofmann auf, der in seiner Darstellung des Gegenstands zunächst die Argumente für ein Ende der Privilegierung darstellt[12], letztlich aber herleitet, warum für eine Auftragsverarbeitung keine eigene Ermächtigung erforderlich ist[13].

Die Begriffsbestimmungen hinsichtlich der Begrifflichkeiten „Verantwortlicher", „Auftragsverarbeiter", „Empfänger" und „Dritter" sind in der Richtlinie 95/46/EG und der DS-GVO nahezu identisch, daher ist es nach Meinung der Autoren nachvollziehbar, dass der Wechsel vom BDSG, welches ja die Richtlinie 95/46/EG umsetzte, zur DS-GVO keine Änderung bzgl. der Interpretation dieser Begrifflichkeiten und der damit verbundenen Privilegierung einer Auftragsverarbeitung beinhaltet. Entsprechend gelten die zur Richtlinie 95/46/EG getroffenen Aussagen der Artikel-29-Datenschutzgruppe auch unter der DS-GVO[14]: Zivilrechtlich ist ein Auftragsverarbeiter kein Dritter und ist - da er nicht zur Partei der Betroffenen zählen kann - somit dem Verantwortlichen zuzurechnen, der ihn auch beauftragt hat. Eine Verarbeitung von Daten eines Betroffenen durch einen Auftragsverarbeiter ist somit - zwar nicht arbeitsrechtlich, wohl aber datenschutzrechtlich - dergestalt zu werten, wie wenn die Verarbeitung statt durch den Auftragsverarbeiter durch einen Mitarbeiter des Verantwortlichen durchgeführt wird. Somit benötigt auch unter den Regelungen der DS-GVO eine Auftragsverarbeitung keinen eigenen Erlaubnistatbestand.

6.2 Wartung / Fernwartung

Im Gegensatz zu § 11 Abs. 5 BDSG ordnet die DS-GVO „die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen" nicht automatisch einer Auftragsverarbeitung zu. Gleichwohl bleiben die in der Vergangenheit mehrfach dargestellten[15] Argumente, aufgrund derer die Prüfung/Wartung, unabhängig davon, ob dies vor Ort oder aus der Ferne (sog. „Fernwartung") geschieht, einer Auftragsverarbeitung zugeordnet werden muss, bestehen. Dies ist insbesondere der Fall, wenn etwa bei Korrekturen aufgrund von Fehlermeldungen oder im Rahmen von Servicearbeiten ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, auch wenn dies zufällig und absichtslos passiert. Beispielsweise kann dies bei folgenden Tätigkeiten eintreten: eine Korrektur (Patch), eine Aktualisierung (Update) oder mitunter auch die Änderung auf eine höhere Version (Upgrade) eines Produktes oder die Reparatur von IT-Anlagen bzw. Geräten durch einen Dienstleister, ohne dass dabei der Dienstleister über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden darf. D. h. der Dienstleister ist kein Verantwortlicher im Sinne der DS-GVO. Dem Wartungsunternehmen werden die personenbezogenen Daten nicht zur eigenen Verarbeitung überlassen, desgleichen erhält das Wartungsunternehmen die Daten nicht zur auftragsgemäßen Verarbeitung im eigentlichen Sinne.

[11] Bayerisches Landesamt für Datenschutzaufsicht (2016) Auftragsverarbeitung nach der DS-GVO. Online, zitiert am 2016-11-04; Verfügbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf

[12] Hofmann J. (2016) §3 Allgemeine Regeln der Datenschutz-Grundverordnung, Rn. 251 in Roßnagel (Hrsg.) Europäische Datenschutz-Grundverordnung. Nomos Verlagsgesellschaft. ISBN 978-3-8487-3074-2

[13] Hofmann J. (2016) §3 Allgemeine Regeln der Datenschutz-Grundverordnung, Rn. 258 in Roßnagel (Hrsg.) Europäische Datenschutz-Grundverordnung. Nomos Verlagsgesellschaft. ISBN 978-3-8487-3074-2

[14] Artikel-29-Datenschutzgruppe. (2010) Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" S. 37f. Online, zitiert am 2016-10-15; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[15] siehe z. B. Büermann U. (1994) Datenschutzrechtliche Einordnung von Wartung und Fernwartung. RDV 202ff oder Müller, Wehrmann R. (1993) Fernwartung und Datenschutz. NJW-CoR 20ff

Gleichwohl bleibt der aus der DS-GVO resultierende Schutzbedarf natürlich unverändert bestehen, sodass der Verantwortliche zwangsläufig für jegliche Wartung, in deren Rahmen ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, einen Auftragsverarbeitungsvertrag entsprechend Art. 28 Abs. 3 DS-GVO mit dem die Wartung durchführenden externen Dienstleister abschließen muss.

Dies gilt nicht nur für die Wartung von Software, sondern auch von Geräten, die personenbezogene Daten speichern. Grundsätzlich muss der Verantwortliche vor der Weitergabe von Geräten, wie medizintechnischen Geräten oder Computern, die darauf gespeicherten Daten löschen. Ggfs. ist aber gerade dies durch einen Defekt des Gerätes nicht möglich, sodass zur Reparatur dieses Gerätes dieses inklusive der darin gespeicherten personenbezogenen Daten an das Wartungsunternehmen übergeben werden muss.

6.3 Auftragsverarbeitung in einem Drittland

Bei der Umsetzung der RL 95/46/EG beschränkte der deutsche Gesetzgeber die Tätigkeit eines Auftragsdatenverarbeiters auf den Geltungsbereich des Europäischen Wirtschaftsraums (§ 3 Abs. 8 S. 3 BDSG). Die RL 95/46/EG kennt diese Beschränkung in den Begriffsbestimmungen nicht, entsprechend fehlt diese territoriale Beschränkung jetzt auch in der DS-GVO.

Aus den expliziten Regelungen für die „Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“ (Kapitel V) ergibt sich, dass die DS-GVO prinzipiell auch eine Übermittlung von Daten in ein Drittland vorsieht. Art. 27 DS-GVO richtet sich dementsprechend explizit an „Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern“. Ein Auftragsverarbeiter kann somit entsprechend den Regelungen der Auftragsverarbeitung sowohl innerhalb der EU als auch in einem Drittland eingesetzt werden. Dies entspricht auch der Intention von Art. 3 Abs. 1 und 2 DS-GVO.

Grundsätzlich kann ein Auftragsverarbeiter in Drittländern nur unter den gleichen Voraussetzungen eingesetzt werden, wie Auftragsverarbeiter innerhalb der EU. Zu beachten sind hierbei insbesondere die zusätzlichen Anforderungen, die einerseits für Auftragsverarbeiter außerhalb der EU gelten (z. B. Art. 28 Abs. 3 S. 3 lit. a DS-GVO) als auch die Anforderungen hinsichtlich der Sicherstellung des Datenschutzniveaus beim Empfänger gemäß Kapitel V DS-GVO.

7 Überprüfung vorhandener ADV-Verträge

Viele Anforderungen der DS-GVO hinsichtlich der vertraglich zu regelnden Pflichten, die nicht explizit in §11 BDSG vorhanden waren, sind in den gängigen Vertragsmustern[16] bereits enthalten, sodass sich – folgte man den Empfehlungen der jeweiligen Verfasser – der Anpassungsbedarf vermutlich in Grenzen hält.

[16] Z. B.
- Bitkom: Aktualisierte Mustervertragsanlage zur Auftragsdatenverarbeitung. Online, zitiert am 2016-09-28; Verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Aktualisierte-Mustervertragsanlage-zur-Auftragsdatenverarbeitung.html),
- GDD-Muster zur ADV gem. § 11 BDSG. Online, zitiert am 2016-09-28; Verfügbar unter https://www.gdd.de/downloads/materialien/muster/Mustervereinbarung%20a7%2011%20BDSG_final1.doc/view),
- ADV-Mustervertrag für das Gesundheitswesen. Online, zitiert am 2016-09-28; Verfügbar unter https://www.gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015)

Zunächst müssen bestehende AV-Regelungen hinsichtlich der Einhaltung der Formvorschrift geprüft werden. In Deutschland hat sich hinsichtlich der ADV überwiegend eine Vertragsgestaltung, wenngleich gesetzlich nicht gefordert, durchgesetzt, sodass in den meisten Fällen ein schriftlicher Vertrag vorhanden sein dürfte.

Weiterhin müssen bestehende ADV-Verträge bzgl. der Pflichten des Auftragsverarbeiters auf ihre Verordnungskonformität geprüft werden, insbesondere hinsichtlich

- der Umsetzung der sicherheitstechnischen Anforderungen der DS-GVO
- der Umsetzung der organisatorischen Anforderungen der DS-GVO
- vorhandener Regelungen zur Vertraulichkeit oder gesetzlichen Verschwiegenheit
- der Bestimmungen bzgl. Unterauftragsverhältnissen
- den Informationspflichten
    - Hinweispflicht seitens des Auftragsverarbeiters bei rechtswidrigen Weisungen durch den Auftraggeber/Verantwortlichen
    - Hinweispflicht des Auftragsverarbeiters bzgl. Übermittlung in ein Drittland
- den Dokumentationspflichten des Auftragsverarbeiters
    - Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten
    - Dokumentationspflicht hinsichtlich der Weisungen
- den Unterstützungspflichten des Auftragsverarbeiters
    - Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber/Verantwortlichen
    - Bei der Zusammenarbeit mit den Aufsichtsbehörden
    - Bei der Meldung von Datenpannen
    - Bei der Datenschutz-Folgenabschätzung
    - Bei Prüfungen durch den Verantwortlichen oder dessen Beauftragten
- des Umgangs mit der Datenverarbeitung in einem Drittland, insbesondere der diesbezüglichen Weisungsabhängigkeit des Auftragsverarbeiters
- der Pflicht zur Rückgabe bzw. Löschung ggfs. vom Auftraggeber erhaltener personenbezogener Daten.

Ferner müssen die Verträge bzgl. der Pflichten des Auftraggebers insbesondere hinsichtlich

- den dokumentierten Weisungsrechten des Verantwortlichen
- der Darlegung der grundsätzlichen Informationen, was in der Auftragsverarbeitung geschehen soll, d. h.
    - Art und Zweck der Verarbeitung
    - Art der personenbezogenen Daten und Kategorien von betroffenen Personen
    - Beschreibung des Auftrags bzw. der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter

überprüft werden.