F.A.Q. zur Auftragsverarbeitung

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Autoren

Bernd Schütze — Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra — Kanzlei Spyra

Stand: 01.05.2017

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

Inhaltsverzeichnis

1 BDSG vs. DS-GVO – Welche grundlegenden Unterschiede bestehen?

1.1 Sprachliche Unterschiede

Erste sprachliche Unterschiede finden sich schon in den von den Gesetzen verwendeten Begrifflichkeiten: So verwendet das BDSG den Begriff „Auftragsdatenverarbeitung“, die europäische Datenschutz-Grundverordnung (DS-GVO) hingegen spricht von „Auftragsverarbeitung“.

Wo das BDSG die Terminologie „Verantwortliche Stelle – Auftragsdatenverarbeiter“ verwendet, heißt es in der DS-GVO „Verantwortlicher“ (Art. 4 Ziff. 7 DS-GVO) und „Auftragsverarbeiter“ (Art. 4 Ziff. 8 DS-GVO). Entsprechend der in der DS-GVO enthaltenen Definition handelt es sich jedoch nach wie vor um die Verarbeitung personenbezogener Daten durch einen Auftragnehmer, d. h. letztlich um eine Datenverarbeitung im Auftrag des Verantwortlichen.

Hinweis: Die heute aktuellen EU Standardvertragsklauseln, welche bis zum Widerruf durch die EU-Kommission oder einem entsprechenden Entscheid des EuGH ihre Gültigkeit behalten (vgl. ErwGr. 171), verwenden wiederum eine andere Terminologie und sprechen von Datenimporteur (= Auftragsverarbeiter) und Datenexporteur (= Verantwortlicher).

1.2 Formale Unterschiede

Wie das BDSG verlangt auch die DS-GVO eine „Regelung“ für eine Auftragsverarbeitung. Nach der DS-GVO kann der Verantwortliche zwischen zwei Möglichkeiten zur Regelung des Verhältnisses zwischen ihm und dem Auftragsverarbeiter („Auftragnehmer“) wählen:

1. Einerseits kann er die vertragliche Form wählen, wie sie bisher in Deutschland in Form von „ADV-Verträgen“ zum Einsatz kam.
2. Darüber hinaus ist nach der DS-GVO bei der Vereinbarung einer Auftragsverarbeitung jedes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zugelassen, welches den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in welchem die Anforderungen der DS-GVO (insbesondere die Anforderungen nach Art. 28 Abs. 3 DS-GVO) geregelt werden.

Die Regelung muss in beiden Fällen schriftlich erfolgen (Art. 28 Abs. 9 DS-GVO), wobei eine elektronische Form auch dem Schriftformerfordernis genügt.

1.3 Sanktionen bei Verstößen

Waren die Sanktionsmöglichkeiten (Bußgelder) bei Verstößen gegen die Regelungen von § 11 BDSG seitens finanzstarker Firmen oder Unternehmen bisher als eher wenig bedeutsam einzuschätzen, hat sich dieses nun mit Geltung der DS-GVO geändert. So drohen gem. Art. 83 DS-GVO bei Verstößen gegen die sich aus Art. 28 DS-GVO ergebenden datenschutzrechtlichen Verpflichtungen sowohl dem Verantwortlichen als auch dem Auftragsverarbeiter Geldbußen in Höhe bis zu 10 Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes des Unternehmens bzw. des Konzerns; je nachdem, welcher Betrag höher ist.

2 Sind alle unter altem Recht abgeschlossenen ADV-Verträge unwirksam? Muss ich einen neuen Vertrag aufsetzen?

Diese Frage kann pauschal nicht beantwortet werden. Es muss jeder Vertrag einzeln geprüft werden, ob er den Anforderungen der DS-GVO genügt. Viele Muster-Vorlagen enthielten über den

Anforderungen des BDSG hinausgehende Empfehlungen. Folgte man diesen Empfehlungen, kann es sein, dass den Anforderungen der DS-GVO mit dem vorhandenen Vertrag genügt wird. Werden die Anforderungen der DS-GVO bereits mit dem existierenden Vertrag erfüllt, ist die Neu-Abschließung nicht erforderlich.

Nur wenn der vorhandene Vertrag nicht allen Anforderungen der DS-GVO entspricht, muss mit einem neuen Vertrag (oder ggf. mit einer Vertragsergänzung bzw. -anpassung) dies geändert werden.

3 Ist jede Verarbeitung nach der DS-GVO eine Auftragsverarbeitung?

Gab es im BDSG nur zwei Formen der „Datenverarbeitung“ durch Externe, nämlich die Datenübermittlung (Funktionsübertragung) und die Auftragsverarbeitung, hat sich auch dieses durch die DS-GVO geändert. So gibt es nun drei Möglichkeiten, wie eine Verarbeitung durch „Externe“ ausgestaltet sein kann:

1. Auftragsverarbeitung
2. Gemeinsame Verarbeitung
3. Funktionsübertragung

Diese Möglichkeiten bieten einem Verantwortlichen einerseits mehr Flexibilität, bedingen andererseits aber auch, den einzelnen Sachverhalt genau zu analysieren, um so die bestmögliche Lösung zu wählen.

Die Möglichkeit der „gemeinsamen Datenverarbeitung“ zeigt zudem auf, dass mit Geltung der DS-GVO nicht jede Verarbeitung in Zusammenarbeit mit anderen (Externen) gleichzeitig immer auch eine Auftragsverarbeitung darstellt.

4 Wie unterscheiden sich die Begriffe?

4.1 Verarbeitung im Auftrag („Auftragsverarbeitung“)

Ähnlich wie bei der Auftragsdatenverarbeitung im BDSG, muss entsprechend Art. 28 DS-GVO auch bei einer „Verarbeitung im Auftrag“ nach der DS-GVO ein Vertrag geschlossen werden.

Auch nach der DS-GVO ist der im Auftrag des Verantwortlichen tätige Dienstleister datenschutzrechtlich kein „Dritter“. Vielmehr nimmt der Dienstleister datenschutzrechtlich wie bisher die Stellung eines „externen Mitarbeiters“ des Verantwortlichen ein. Dieses wiederum hat zur Konsequenz, dass die „Verarbeitung im Auftrag“ von den aus Artt. 6 bis 11 resultierenden Legitimationen der Verarbeitung des Verantwortlichen gedeckt ist und deshalb grundsätzlich auch kein eigener Erlaubnistatbestand für die Auftragsverarbeitung erforderlich ist.

Wenngleich die Verantwortung für die Rechtmäßigkeit der Verarbeitung beim Verantwortlichen liegt (vgl. Art. 5 Abs. 2 DS-GVO), weist die DS-GVO dem Auftragsverarbeiter auch eigene Pflichten zu, denen dieser genügen muss. Somit kann ein Verstoß gegen diese Pflichten direkt gegen den Auftragsverarbeiter geltend gemacht werden, ohne dass der Verantwortlichen zunächst in Regress genommen werden muss.

4.2 Funktionsübertragung

Der Begriff der Funktionsübertragung findet sich häufig sowohl in der juristischen in Literatur wie auch in der Rechtsprechung wieder auch wenn dieser Begriff nicht legaldefiniert ist. So sucht man diesen Begriff vergeblich in den einschlägigen Datenschutzgesetzen wie dem BDSG, den kirchlichen- oder den Landesgesetzen und auch nicht in der EU-Richtlinie 95/46/EG. In der DS-GVO ist dieser Begriff ebenfalls nicht definiert.

Der Begriff der Funktionsübertragung wurde zum ersten Mal 1989 in der Gesetzesbegründung zum BDSG erwähnt[1]. Darin heißt es:

> „Wie bisher handelt es sich nicht um Auftragsdatenverarbeitung im Sinne dieser Vorschrift, wenn neben der Datenverarbeitung auch die zugrundeliegende Aufgabe übertragen wird (Funktionsübertragung). In diesem Falle hat derjenige, dem die Funktion übertragen wird, alle datenschutzrechtlichen Pflichten, insbesondere die Ansprüche des Betroffenen, zu erfüllen.

In diesem Sinne existiert die Funktionsübertragung bis heute und wird auch mit Wirkung der DS-GVO weiter fortbestehen, selbst wenn keine diesbezügliche Legaldefinition existiert. Wie durch die Gesetzesbegründung deutlich wird, stellt die Funktionsübertragung im Prinzip lediglich die Verarbeitung personenbezogener Daten durch einen Dritten dar, wobei dieser Dritte bei der Verarbeitung der Daten selbst über Datenverarbeitungszwecke und -mittel zur Erfüllung der ihm übertragenen / vereinbarten Aufgabe entscheidet. Damit ist dieser Dritte selbst vollumfänglich für die Verarbeitung fremder Daten verantwortlich und im Sinne der DS-GVO daher ein „Verantwortlicher".

Auch die DS-GVO sagt in Art. 28 Abs. 10 DS-GVO, dass ein Auftragsverarbeiter, der die Daten des Verantwortlichen verarbeitet und dabei selber über die Mittel und Zwecke dieser Verarbeitung entscheidet, als Verantwortlicher zu qualifizieren ist; dies gilt selbstverständlich auch im Sinne einer Funktionsübertragung.

4.3 Gemeinsame Verarbeitung („Joint controllers")

Anders als bspw. das BDSG kennt die DS-GVO eine gemeinsame Verantwortlichkeit bei einer Datenverarbeitung. Dies verdeutlicht die Begriffsbestimmung des „Verantwortlichen" in Art. 3 Ziff. 7 DS-GVO, in der es heißt:

> „die 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".

Diesem Wortlaut folgend, muss ein Verantwortlicher damit nicht zwingend eine einzige natürliche oder juristische Person sein, wie es beim BDSG hinsichtlich der verantwortlichen Stelle der Fall war. Vielmehr kann „der Verantwortliche" auch aus mehreren Parteien bestehen, die sich gemeinsam die Verantwortung bzgl. der Verarbeitung der personenbezogenen Daten teilen. Art. 26 DS-GVO nennt die Voraussetzungen, unter welchen Umständen eine solche gemeinsame Verarbeitung statthaft ist.

[1] Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (6. April 1989) Begründung zu Artikel 1 (Bundesdatenschutzgesetz, Abschnitt §10 „Verarbeitung personenbezogener Daten im Auftrag". [Online, zitiert am 2017-04-02]; Verfügbar unter https://dipbt.bundestag.de/doc/btd/11/043/1104306.pdf

4.3.1 Gemeinsame Verarbeitung– Was muss beachtet werden?

Existiert bei der Datenverarbeitung mehr als ein Verantwortlicher, so muss nach Art. 26 DS-GVO eine entsprechende Vereinbarung in „transparenter Form“ regeln (Art. 26 Abs. 1 DS-GVO):

- wer von den Verantwortlichen, welche der Vorgaben / Aufgaben der DS-GVO erfüllt,
- wer für die Wahrnehmung / Erfüllung der Betroffenenrechte verantwortlich ist und
- wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt.

Desgleichen müssen in der Vereinbarung sowohl die Art, die (Begleit-) Umstände, als auch die Mittel der Verarbeitung festlegt werden. D. h. es ist eine genaue Beschreibung hinsichtlich der Aufgaben zwischen den beteiligten Verantwortlichen erforderlich, in welcher insbesondere aufgeführt wird:

1. Eine Darstellung, welche der Parteien an der gemeinsamen Verarbeitung beteiligt sind.
2. Die Festlegung des Zwecks bzw. der Zwecke der Datenverarbeitung.
3. Eine Darstellung der Mittel hinsichtlich der Datenverarbeitung. Dieses beinhaltet insbesondere auch, welcher der Verantwortlichen wie und in welchem Umfang für die Entscheidung welcher Mittel verantwortlich ist.
4. Die Pflichten der Verantwortlichen, insbesondere auch hinsichtlich der Klärung der Frage, wer für die Gewährleistung von welchen Betroffenenrechten verantwortlich ist.
5. Eine Darstellung, wer welche Informationspflichten wahrnimmt im Rahmen
    a. der Datenerhebung (Artt. 13, 14 DS-GVO),
    b. bei Anfragen Betroffener,
    c. bei der Be- bzw. Verarbeitung von Betroffenendaten im Sinne von Korrektur, Sperrung, Löschung usw.,
    d. bei der Meldung von Datenpannen.

5 Auftragsverarbeitung, gemeinsame Verarbeitung, Funktionsübertragung – Wo sind die Unterschiede?

Die nachfolgende Tabelle soll überblicksartig darstellen, wo die Unterschiede zwischen der „Auftragsverarbeitung“, der „gemeinsamen Verarbeitung“ und der Funktionsübertragung liegen.

	Auftragsverarbeitung	Gemeinsame Verarbeitung	Funktionsübertragung
Grundsatz	Weisungsgebundene Verarbeitung von Daten durch Auftragnehmer	(Gleichberechtigte) Partnerschaft mit gemeinsamer Verantwortung	Eigenverantwortliche Entscheidung des Auftragnehmers über die Art und Weise der Datenverarbeitung
Erlaubnistatbestand	Verantwortlicher verfügt über einen Erlaubnistatbestand für die Verarbeitung, der gleichzeitig die Auftragsdatenverarbeitung legitimiert.	Die gemeinsam an der Verarbeitung Beteiligten haben einen (gemeinsamen) Erlaubnistatbestand	Verantwortlicher hat einen Erlaubnistatbestand zur Übermittlung der Datenverarbeitung / der Verarbeitungsaufgabe an den anderen Verantwortlichen
Voraussetzung für	Vertrag oder sonstiges	Aufteilung der	Die datenempfangende

Verarbeitung	Rechtsinstrument entsprechend Art. 28 DS-GVO	Pflichten gemäß Art. 26 (und entsprechende vertragliche Regelung / Vereinbarung)	Partei braucht einen eigenen Erlaubnistatbestand zur Datenverarbeitung.
Beispiel	Verantwortlicher beauftragt Hersteller mit Wartung und Weiterentwicklung von Software	Krankenhaus und MVZ behandeln gemeinsam einen Patienten	Laborarzt empfängt Daten vom Hausarzt zur Laboruntersuchung

6 Umgang mit Unterauftragnehmern

6.1 Ist jede vom Auftragnehmer beauftragte Fremdleistung ein Unterauftragnehmer?

Die Fragestellung, ob jede vom Auftragnehmer beauftragte Fremdleistung (im Rahmen der Auftragsverarbeitungstätigkeiten für den Verantwortlichen) eine „Unterbeauftragung“ sein kann, lässt sich grundsätzlich mit einem „Nein“ beantworten.

Entscheidend ist, ob ein Zugriff durch den vom Auftragsverarbeiter Beauftragten auf personenbezogene Daten des Verantwortlichen erfolgt oder etwa durch entsprechende Schutzmaßnahmen ein Zugriff ausgeschlossen werden kann. Wenn kein Zugriff auf die personenbezogenen Daten des Verantwortlichen (i.S. des Auftraggebers des Auftragsverarbeiters) möglich ist, z. B. weil der Auftragsverarbeiter mittels technischer und/oder organisatorischer Maßnahmen gewährleistet, dass kein (rechtskonformer) Zugriff erfolgen kann, liegt die Beauftragung mangels Verarbeitung personenbezogener Daten außerhalb des Geltungsbereichs der DS-GVO.

Jedoch muss hierbei immer beachtet werden, dass schon die Kenntnisnahme personenbezogener Daten eine Verarbeitung darstellt. (Siehe zu dieser Thematik auch Abschnitt 9.2)

7 Verantwortlichkeit

7.1 Wer ist für die Verarbeitung verantwortlich?

Auch in der DS-GVO ist grundsätzlich – wie im BDSG – der für die Verarbeitung Verantwortliche und nicht der Auftragsverarbeiter für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich. Insbesondere ist der Verantwortliche dafür zuständig, zu gewährleisten, dass eine Verarbeitung personenbezogener Daten nur aufgrund eines legitimen Erlaubnistatbestandes erfolgt (vgl. auch die Grundsätze in Art. 5 Abs. 1 DS-GVO, für deren Einhaltung entsprechend Art. 5 Abs. 2 DS-GVO der Verantwortliche verantwortlich und rechenschaftspflichtig ist).

7.2 Wer entscheidet über die Verarbeitung?

Die Definition des Auftragsverarbeiters in Art. 4 Ziff. 8 DS-GVO stellt lediglich auf ein Auftragsverhältnis zwischen Verantwortlichen und Auftragsverarbeiter ab. Durch die Legaldefinition ist damit grundsätzlich ein gewisses eigenverantwortliches Handeln und ein angemessener Entscheidungsspielraum des Auftragsverarbeiters möglich, solange sich diese Verarbeitung noch in

den Grenzen des Art. 28 DS-GVO bewegt. Eine zulässige Auftragsverarbeitung ist deshalb nur unter Einhaltung der Vorgaben dieses Artikels möglich.

So verlangt bspw. Art. 28 Abs. 3 S. 2 lit. a DS-GVO, dass „die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen“ durch den Auftragsverarbeiter verarbeitet werden dürfen. Auch Art. 29 DS-GVO, der sich mit den Pflichten der vom Auftragsverarbeiter zur Auftragserfüllung eingesetzten Personen auseinandersetzt, stellt deutlich heraus, dass eine Verarbeitung nur auf Weisung des Verantwortlichen erfolgen darf.

Dieses wiederum hat zur Konsequenz, dass ein eigenverantwortliches Handeln des Auftragsverarbeiters bzw. der von ihm im Rahmen des Auftragsverarbeitungsverhältnisses eingesetzten Personen, nur im Rahmen der Vorgaben des Verantwortlichen möglich ist. Der Auftragsverarbeiter ist somit wie eine beschäftigte Person des Verantwortlichen anzusehen, die auch nur im Rahmen ihres Dienstverhältnisses tätig werden darf, in diesem aber einen gewissen Entscheidungsspielraum zur Verfügung hat.

7.3 Wer haftet bei Datenschutzverstößen?

Im Gegensatz zum BDSG haften entsprechend Art. 82 DS-GVO sowohl Verantwortlicher als auch Auftragsverarbeiter für Verstöße gegen die Vorgaben der DS-GVO. So kann sich dieser Regelung folgend eine betroffene Person, welcher durch einen Verstoß gegen die DS-GVO ein materieller oder immaterieller Schaden entsteht, hinsichtlich etwaiger Schadensersatzansprüche gemäß Art. 82 Abs. 1 DS-GVO sowohl an den Verantwortlichen wie auch an den Auftragsverarbeiter wenden.

Wie in Kapitel 1.3 angesprochen können gemäß Art. 83 Abs. 3 DS-GVO Aufsichtsbehörden bei Datenschutzverstößen Bußgelder sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter verhängen.

8 Welche (neuen) Pflichten hat der Auftragsverarbeiter?

Durch die DS-GVO kommen auf einen Auftragsverarbeiter neue Pflichten zu. Einige dieser Pflichten werden im Nachfolgenden kurz dargestellt.

8.1 Gewährleistung der Sicherheit der Verarbeitung

Gemäß Art. 32 Abs. 1 müssen sowohl der Verantwortliche als auch der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, welche ein dem Risiko angemessenes Schutzniveau gewährleisten. Dabei hat die Verarbeitung von besonderen Kategorien personenbezogener Daten (Art. 9 DS-GVO) wie etwa Gesundheitsdaten automatisch zur Konsequenz, dass ein sehr hohes Schutzniveau gewährleistet werden muss.

8.2 Verzeichnis über Verarbeitungstätigkeiten

Entsprechend Art. 30 Abs. 2 DS-GVO sind Auftragsverarbeiter verpflichtet, ein Verzeichnis über die Verarbeitungstätigkeiten, welche sie für einen Verantwortlichen („Auftraggeber“) übernehmen, zu führen. Dieses Verzeichnis muss mindestens die in Art. 30 DS-GVO geforderten Angaben konkret abbilden.

8.3 Meldepflichten

Entsprechend Art. 33 Abs. 2 DS-GVO muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden, damit dieser dann entsprechend seiner gesetzlichen Verpflichtungen tätig werden kann.

9 Besondere Fragestellungen

9.1 Bleibt die Privilegierung erhalten?

Die Auftragsverarbeitung wird in Deutschland derzeit praktisch durchgehend als „privilegierter" Tatbestand betrachtet, bei der die Weitergabe von Daten vom Verantwortlichen an den Auftragsverarbeiter keiner weiteren gesetzlichen Rechtfertigung bedarf. Dieses wird u.a. daraus abgeleitet, dass § 3 Abs. 4 Ziff. 3 BDSG klarstellt, dass eine „Weitergabe" an den Auftragsdatenverarbeitungsnehmer keine Übermittlung im Sinne von § 3 Abs. 4 Ziff. 3 BDSG darstellt, da der Auftragnehmer (Auftragsverarbeiter) entsprechend § 3 Abs. 8 S. 3 BDSG kein Dritter im Sinne des Gesetzes ist.

Die Begriffsbestimmungen hinsichtlich der Begrifflichkeiten „Verantwortlicher", „Auftragsverarbeiter", „Empfänger" und „Dritter" in der Richtlinie 95/46/EG, die maßgeblich die Begriffsbestimmungen des BDSG geprägt haben, sind in der DS-GVO nahezu identisch vorhanden. Daraus lässt sich schlussfolgern, dass sich durch den Wechsel vom BDSG, welches ja die Richtlinie 95/46/EG umsetzte, zu den Regelungen der DS-GVO keine Änderung hinsichtlich der Interpretation dieser Begrifflichkeiten und der damit verbundenen Privilegierung einer Auftragsverarbeitung ergibt. Konsequenterweise müssen daher die von der Art. 29-Datenschutzgruppe zur Richtlinie 95/46/EG getroffenen Aussagen auch mit Geltung der DS-GVO[2] weiterhin Anwendung finden. So stellt die Art. 29-Gruppe in dem vorstehend zitierten Dokument heraus, dass schon zivilrechtlich der Auftragsverarbeiter kein Dritter, sondern vielmehr Erfüllungs- (§ 278 BGB) bzw. Verrichtungsgehilfe (§ 831 BGB) ist. Daher ist er auch keine Partei des Betroffenen sondern muss (haftungsrechtlich) dem Verantwortlichen zugerechnet werden, der ihn auch beauftragt hat.

Eine Verarbeitung von Daten eines Betroffenen durch einen Auftragsverarbeiter ist somit - zwar nicht arbeitsrechtlich, wohl aber datenschutzrechtlich - auch nach der DS-GVO dergestalt zu werten, als wenn die Verarbeitung statt durch den Auftragsverarbeiter durch einen Mitarbeiter des Verantwortlichen vorgenommen wird. Somit gilt auch mit Wirkung der Regelungen der DS-GVO, dass eine Auftragsverarbeitung als „privilegierte Verarbeitung" keinen eigenen Erlaubnistatbestand benötigt.

9.2 § 11 Abs. 5 BDSG fällt weg: Wie ist aus Sicht der DS-GVO mit der „Wartung" umzugehen?

Im Gegensatz zu § 11 Abs. 5 BDSG sieht die DS-GVO „die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen" nicht automatisch als Auftragsverarbeitung an.

[2] 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

Gleichwohl bleiben die schon in den 1990er Jahren mehrfach vorgetragenen [3] und von der juristischen Literatur immer wieder aufgegriffenen Argumente, aufgrund derer die Prüfung/Wartung einer Auftragsverarbeitung zugeordnet werden muss, auch unabhängig davon, ob dies vor Ort oder aus der Ferne (sog. „Fernwartung“) geschieht, , bestehen.

Die Regelungen zur Auftragsverarbeitung gelten insbesondere immer dann, 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.

Ohne einen bestehenden, wirksamen Vertrag (oder anderem Rechtsinstrument der EU) zur Auftragsverarbeitung, sind mithin natürliche oder juristische Personen, welche Kenntnis von den zu schützenden personenbezogenen Daten erhalten, Dritte im datenschutzrechtlichem Sinne. Entsprechend der Vorgaben der DS-GVO muss daher für die Weitergabe der Daten vom Verantwortlichen an diesen Dritten ein Erlaubnistatbestand vorliegen. Ferner muss der „Dritte“ (im Sinne einer Funktionsübertragung) als Verantwortlicher für diese Daten die entsprechend einem Verantwortlichen obliegenden Pflichten erfüllen.

Bei „normalen“ Daten dürfte in diesen Fällen regelmäßig der Erlaubnistatbestand (auch ohne einen Auftragsdatenverarbeitungsvertrags) der Übermittlung / Verarbeitung des Art. 6 Abs. 1 lit. f DS-GVO einschlägig sein, weil das Interesse des Verantwortliche an der Wartung des Systems ein berechtigtes Interesse im Sinne dieser Vorschrift darstellt. Eine Kenntnisnahme von personenbezogenen Daten durch die die Wartung durchführende Person (wenn entsprechende Schutzmaßnahmen getroffen wurden) dürfte nur in Ausnahmefällen erfolgen.

Bei einem solchen Zugriff sollten ferner i.d.R., u.a. auch weil entsprechende technische und organisatorische Maßnahmen getroffen wurden, auch nur eine geringe Teilmenge der Daten betroffen sein. In der Gesamtschau dürfte deshalb in solchen Fällen das Interesse des Verantwortlichen das Interesse des Betroffenen am Schutz der ihn betreffenden Daten überwiegen bzw. das Betroffeneninteresse dürfte dem Interesse des Verantwortlichen nicht maßgeblich entgegenstehen.

Wie vorstehend angemerkt, gehören aber gerade Gesundheits- oder Sozialdaten zu den besonderen Kategorien personenbezogener Daten, deren Verarbeitung ausschließlich nur mittels der in Art. 9 DS-GVO aufgeführten Erlaubnistatbestände legitimiert werden kann. Art. 9 DS-GVO kennt keinen mit Art. 6 Abs. 1 lit. f DS-GVO vergleichbaren Erlaubnistatbestand, sodass in der Konstellation, in der kein wirksamer Auftragsdatenverarbeitungsvertrag abgeschlossen wurde, letzten Endes nur die Möglichkeit bleibt, die wirksame, ausdrückliche Einwilligung der betroffenen Person(en) einzuholen, was aufgrund der mannigfaltigen „Hürden“, die es bei einer Einwilligung zu beachten gilt[4], letztlich in der Praxis nicht umsetzbar ist.

Um den vorstehend beschriebenen Problemen aus dem Wege zu gehen, verbleibt für den Fall, dass ein Zugriff auf zu schützende personenbezogene Daten durch einen Dienstleister nicht

[3] 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

[4] Zu den datenschutzrechtlichen Anforderungen der DS-GVO an die Einwilligung siejhe auch die Ausarbeitung der GMDS, online verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/einwilligung.php

auszuschließen ist, realistischer Weise nur die Möglichkeit, bei derartigen Arbeiten einen den Anforderungen der DS-GVO genügenden Vertrag zur Auftragsdatenverarbeitung abzuschließen

9.3 Ist jetzt eine Auftragsverarbeitung in der ganzen Welt erlaubt?

Aus den Regelungen der DS-GVO (Kapitel V - „Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“) ergibt sich, dass prinzipiell auch eine Auftragsverarbeitung / Übermittlung von Daten in einem Drittland (bei Vorliegen entsprechender Garantien) möglich ist.

Dieses wird bspw. auch durch den Wortlaut von Art. 27 DS-GVO deutlich. So richtet sich dieser Art. explizit an Verantwortliche und Auftragsverarbeiter außerhalb der EU, was wiederum impliziert, dass die DS-GVO eine Auftragsverarbeitung außerhalb der EU durchaus als zulässig ansieht. Ein Auftragsverarbeiter kann somit entsprechend der DS-GVO-Regelungen sowohl innerhalb der EU als auch in einem Drittland eingesetzt werden. Diese Sichtweise wird u.a. auch durch den Wortlaut des Art. 3 Abs. 1 und 2 DS-GVO untermauert, der die Anwendbarkeit der DS-GVO Regelungen auch auf die Auftragsverarbeitung in einem Drittland erstreckt.

Daher muss die Frage, ob nun auch die Auftragsverarbeitung in einem Drittland möglich ist, grundsätzlich mit einem „Ja“ beantwortet werden.

Allerdings muss bei der Beauftragung eines Auftragsverarbeiters in einem Drittland beachtet werden, dass dieser nur beauftragt werden darf, wenn in diesem Drittland die Verarbeitung unter den gleichen Voraussetzungen – insbesondere hinsichtlich der Sicherheit der Daten - erfolgt, als wenn die Verarbeitung durch einen Auftragsverarbeiter innerhalb der EU erfolgen würde.

Dieses hat mithin zur Konsequenz, dass Auftragsverarbeiter in Ländern, in denen kein der EU vergleichbares Schutzniveau für die Betroffenendaten existiert grundsätzlich dann nicht beauftragt werden dürfen, wenn nicht sichergestellt ist, dass die Verarbeitung der Daten „sicher“ und konform mit den Regelungen der DS-GVO erfolgen kann.

10 Fragen aus der Praxis: Was ist eigentlich …?

10.1 Archivierungsdienste

Ist ein Zugriff auf personenbezogene Daten nicht ausgeschlossen, liegt eine Auftragsverarbeitung vor.

10.2 Backup-Dienstleister

Ist ein Zugriff auf personenbezogene Daten nicht ausgeschlossen, liegt eine Auftragsverarbeitung vor.

10.3 Home Office

Auch wenn ein Beschäftigter eines Unternehmens zu Hause arbeitet, erfolgt die Verarbeitung in einem Unternehmen; es liegt daher weder eine Auftragsverarbeitung noch eine Funktionsübertragung vor. Daher muss auch kein eigenständiger Vertrag diesbezüglicher abgeschlossen werden.

Erfolgt die Verarbeitung hingegen durch einen externen Auftragnehmer oder einen Selbstständigen, so muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden.

10.4 Leih- / Zeitarbeitnehmer

Leih- und Zeitarbeitnehmer stehen im Rahmen einer Arbeitnehmerüberlassung den Beschäftigten eines Unternehmens gleich, daher liegt hier weder eine Funktionsübertragung noch eine Auftragsverarbeitung vor.

10.5 Miete fremder Datenverarbeitungsanlagen / Rechenkapazität

Wenn der Vermieter- i.d.R. das Rechenzentrum – (laut Vertrag oder durch technische Maßnahmen bedingt) keinen Zugriff auf die Daten hat, liegt nur ein Mietverhältnis und keine Verarbeitung personenbezogener Daten vor.

Ist ein Zugriff auf personenbezogene Daten nicht ausgeschlossen, liegt eine Auftragsverarbeitung vor.

10.6 Personalvertretung (Personalrat, Betriebsrat, …)

Eine Weitergabe von Daten an die Personalvertretung des Unternehmens gilt als Datennutzung innerhalb des Unternehmens.

Eine Weitergabe personenbezogener Daten an die Personalvertretung eines anderen Konzernunternehmens, den Gesamt- oder Konzernbetriebsrat ist hingegen eine Übermittlung und ist – je nach Aufgabengestaltung eine Funktionsübertragung oder eine Auftragsverarbeitung.

10.7 Schreibbüro

Ist die Kenntnisname zu schützender personenbezogener Daten nicht ausgeschlossen, liegt wahrscheinlich

a) eine Auftragsverarbeitung vor, wenn nur vorformulierte Texte verarbeitet werden
b) eine Funktionsübertragung vor, wenn selbstständig Texte erstellt werden.

10.8 Übersetzungsbüro

Ist die Kenntnisname zu schützender personenbezogener Daten nicht ausgeschlossen, liegt wahrscheinlich

a) eine Auftragsverarbeitung vor, wenn nur vorformulierte Texte verarbeitet werden
b) eine Funktionsübertragung vor, wenn selbstständig Texte erstellt werden.

10.9 Wartungsarbeiten

Ist ein Zugriff auf personenbezogene Daten nicht ausgeschlossen, liegt eine Auftragsverarbeitung vor.