# Auftragsdatenverarbeitung
# Verantwortlichkeiten des Auftraggebers und des Auftragnehmers

**Stand: 07.02.2018**

## I. Auftragsdatenverarbeitung

Mit Inkrafttreten von EU-DSGVO und neuem BDSG am 25.05.2018 gelten neue Regelungen auch für die Auftragsverarbeitung (AV). Für Auftraggeber einer AV führt dies nicht zu grundlegenden Änderungen, da ihre Obliegenheiten weitestgehend dem bisherigen § 11 BDSG entsprechen. Die Auftragnehmer werden dagegen deutlich stärker in die Pflicht genommen.

AV ist die Verarbeitung personenbezogener Daten durch einen Dienstleister ausschließlich (!) auf Weisung eines Auftraggebers. Es handelt sich mithin um unterstützende Tätigkeit für eine Datenverarbeitung des Auftraggebers. Die AV ist daher von einer anderweitigen Übermittlung von Daten an Dritte bzw. einer (auch) eigenverantwortlichen Datenverarbeitung durch Dritte - etwa beim Inkasso - abzugrenzen. Relevanz für die Praxis hat die AV besonders bei der Einschaltung externer Dienstleister etwa in den Bereichen Honorarabrechnung, Terminvergabe, Marketing, EDV (z.B. Systembetreuung/-wartung, Vernichtung von Datenträgern, "Cloud-Computing"), Lohnabrechnung etc.

Ob eine AV - mit den entsprechenden Rechtsfolgen - vorliegt, richtet sich ausschließlich nach den gesetzlichen Vorgaben, kann also nicht vertraglich festgelegt/ ausgeschlossen werden. Denn im Falle einer AV ist die Übermittlung der Daten an den Dienstleister insofern "privilegiert", als sie nicht den üblichen Anforderungen unterliegt und hierfür keine gesetzliche Erlaubnis oder gesonderte Einwilligung des Betroffenen erforderlich ist. Dafür müssen andererseits bestimmte rechtliche Anforderungen beachtet und Pflichten erfüllt werden.

Liegt eine AV vor, muss zwinge nd ein Vertrag in schriftlicher oder elektronischer Form geschlossen werden, der die Vorgaben des Art. 28 Abs. 3 DSGVO erfüllt. Ein ausführlich kommentiertes Muster, das auf die besonderen Belange des Gesundheitswesens eingeht, ist unter www.daebl.de/CS39 erhältlich.

Der Auftraggeber hat den Dienstleister ("Auftragsverarbeiter") sorgfältig und unter Berücksichtigung der Gewährleistung geeigneter technischer und organisatorischer Maßnahmen für einen ausreichenden Datenschutz auszuwählen. So treffen ihn vor Vertragsschluss und auch während der Laufzeit (Art. 32 Abs. 1 lit. d DSGVO) gewisse Kontroll- und Dokumentationspflichten. In der Regel ist hierfür die Vorlage aktueller Dokumente ausreichend, aus denen sich ergibt, dass der Auftragsverarbeiter geeignet ist und die gesetzlichen Anforderungen erfüllt (z.B. durch Zertifizierungen). Ohne Genehmigung darf der Dienstleister keinen weiteren Auftragsverarbeiter einschalten.

## II. Verantwortlichkeiten

Bei der AV bleibt Verantwortung für die Einhaltung datenschutzrechtlicher Vorgaben grundsätzlich bei dem Auftraggeber ("Verantwortlicher"). Er ist daher auch Ansprechpartner für die von der Datenverarbeitung betroffenen Personen und verantwortlich bezüglich der den Betroffenen nach Art. 12 bis 23 DSGVO und §§ 32 ff. BDSG-neu zustehenden Rechte wie Auskunft, Berichtigung, Löschung etc. Der Auftragsverarbeiter hat den Verantwortlichen hierbei aber ggf. ebenso zu unterstützen wie bei Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO; beides ist auch zwingend vertraglich zu regeln.

Soweit der Auftragsverarbeiter allerdings gegen die vertraglich festgelegte Datenverarbeitung bzw. gegen Weisungen des Verantwortlichen verstößt, indem er die Zwecke und Mittel der Verarbeitung selber bestimmt, gilt er selber als Verantwortlicher (Art. 28 Abs. 10 DSGVO).

Verantwortlicher und Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Datenschutzniveau zu gewährleisten. Dies beinhaltet vor allem die in Art. 32 DSGVO und (bei Verarbeitung "besonderer Kategorien" von Daten wie Gesundheitsdaten) in § 22 Abs. 2 BDSG-neu genannten Maßnahmen. Im Rahmen einer AV gilt dies sowohl hinsichtlich der Erbringung der AV an sich (z.B. externe Honorar- oder Lohnabrechnung) als auch den dafür erforderliche Datentransfer an den Auftragsverarbeiter. Der bzw. die jeweiligen Datenschutzbeauftragten sind in alle Fragen frühzeitig einzubinden. Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, hat er diese dem Verantwortlichen unverzüglich zu melden (Art. 33 Abs. 2 DSGVO).

## III. Haftung, Bußgelder

Für materielle oder immaterielle Schäden infolge eines Verstoßes gegen die DSGVO haftet im Außenverhältnis jeder Verantwortliche und jeder beteiligte Auftragsverarbeiter zunächst gemeinsam für den gesamten Schaden (Art. 82 Abs. 1, Abs. 4 DSGVO).

Wer nachweist, dass er "in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art. 82 Abs. 3 DSGVO), ist von der Haf-

tung befreit. Wer Schadenersatz gezahlt hat, kann im Innenverhältnis von den übrigen beteiligten Verantwortlichen oder Auftragsverarbeitern den Teil zurückzufordern, der dem jeweiligen Verantwortungsanteil entspricht. Die Haftung des Auftragsverarbeiters beschränkt sich dabei allerdings auf Verstöße gegen speziell ihm gesetzlich auferlegte Pflichten oder für Schäden infolge der Nichtbeachtung oder des Zuwiderhandelns gegen Anweisungen des Verantwortlichen.

Empfindlich verschärft wurden die Bußgeldandrohungen. Bei Verstößen gegen die gesetzlichen Pflichten drohen Verantwortlichen und Auftragsverarbeitern nach Art. 83 Abs. DSGVO Geldbußen von bis zu 20 Millionen Euro oder 2% des Jahresumsatzes.

**IV. Beachtung der Schweigepflicht**

Im Zusammenhang mit der AV ist darauf hinzuweisen, dass auch der Straftatbestand der Verletzung der ärztlichen Schweigepflicht (§ 203 StGB) Ende 2017 geändert bzw. ergänzt wurde. Das Heranziehen externer Dienstleister war nach der vorherigen Fassung nicht ohne strafrechtliches Risiko, sofern der Dienstleister dadurch von geschützten Geheimnissen erfahren konnte – was nicht selten (z.B. bei der EDV-Wartung oder Aktenvernichtung) der Fall ist.

Nach der Neufassung des § 203 StGB ist es nun nicht mehr strafbar, ein geschütztes Geheimnis gegenüber Personen zu offenbaren, "die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit […] erforderlich ist". Dafür werden andererseits die "mitwirkenden Personen" in die Strafbarkeit mit einbezogen, sofern sie selber geschützte Geheimnisse unbefugt offenbaren. Den "Berufsgeheimnisträgern" (Arzt, Zahnarzt etc.) sind wiederum Sorgfaltspflichten auferlegt, welche die Verschwiegenheit der mitwirkenden Personen sicherstellen sollen; insbesondere müssen diese zur Geheimhaltung verpflichtet werden. Es ist unbedingt zu empfehlen, dies zu dokumentieren.

Selbstverständlich sind daneben die berufsrechtlichen Regelungen zur Schweigepflicht zu beachten, die unter Umständen, allerdings eher in Ausnahmefällen, strenger sein können.

**V. Praxishinweis**

Es besteht keine grundsätzliche Pflicht, bisher bereits abgeschlossene Vereinbarungen zur AV zu ersetzen, sofern diese bereits alle inhaltlichen und formalen Anforderungen der DSGVO erfüllen. Geboten ist jedoch, diese dementsprechend und unter Hinzuziehung des Auftragsverarbeiters zu prüfen - die hieran schon angesichts der sie neu treffenden Haftung Interesse haben dürften.

**Anlage:**

**DSGVO, Erwägungsgrund 81**

Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

**Art. 4 Nr. 8 DSGVO**

Im Sinne dieser Verordnung bezeichnet der Ausdruck [...] Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

**Art. 28 DSGVO – Auftragsverarbeiter**

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c)alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d)die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f)unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g)nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

h)dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines an-

deren Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

**Art. 29 DSGVO - Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters**

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

**Art. 32 DSGVO - Sicherheit der Verarbeitung**

(1) 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 Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a)die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b)die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c)die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d)ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

**Artikel 82 - Haftung und Recht auf Schadenersatz**

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein 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 oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen,die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.