AUFTRAGSVERARBEITUNG

Juni 2020
Prof. Dr. Anne Riechert

Rechtsgrundlage:

Artikel 28 Datenschutzgrundverordnung und Erwägungsgrund 81

A. Voraussetzungen

Das Instrument der Auftragsverarbeitung ist wie unter dem bisherigen Recht insbesondere für Outsourcing-Verträge relevant. Beispiele sind etwa Verträge im Rahmen von Cloud-Computing, der Newsletterversand, die Auslagerung von Lohn- und Gehaltsabrechnungen oder Backup-Datenspeicherungen:

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, wobei Verantwortlicher der Datenverarbeitung nach der Datenschutzgrundverordnung derjenige ist, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Artikel 4 Abs. 7 DSGVO). Der Auftragsverarbeiter ist -wie bisher- nach den Regelungen der Datenschutzgrundverordnung weisungsgebunden.

Im Falle einer gesonderten vorherigen Zustimmung des Verantwortlichen darf ein Auftragsverarbeiter jedoch selbst Subunternehmer unter der Voraussetzung beauftragen, dass diesen dieselben Datenschutzpflichten auferlegt und insbesondere hinreichende Garantien hinsichtlich der geeigneten technischen und organisatorischen Maßnahmen geboten werden (siehe hierzu die Regelungen des Artikel 28 Absatz 2 und Absatz 4 DSGVO).

Neu ist im Gegensatz zur (bis Mai 2018 geltenden) Rechtslage, dass die Datenschutzgrundverordnung dem Auftragsverarbeiter mehr Rechtspflichten auferlegt (z.B. Verzeichnis für Verarbeitungstätigkeiten) und zudem Haftungsregelungen bei Datenschutzverletzungen enthält.

Außerdem kann nun auch mit einem Dienstleister, der seinen Geschäftssitz außerhalb der Europäischen Union hat, ein Vertrag zur Auftragsverarbeitung geschlossen werden. Unter bisherigem Recht wurde dies seitens der Aufsichtsbehörden abgelehnt, da in einem solchen Fall der Auftragnehmer stets als „Dritter" eingeordnet wurde, so dass keine *Auftragsdatenverarbeitung (= Begriff des BDSG-alt)* in Betracht kam sondern eine Übermittlung von Daten (an einen Dritten), deren Zulässigkeit an bestimmte rechtliche Voraussetzungen geknüpft war (z.B. die Einwilligung der Betroffenen, Sicherstellung eines angemessenen Schutzniveaus oder Abschluss von Standardvertragsklauseln). Aufgrund der Weisungsgebundenheit des Auftragsverarbeiters wurde bei einer Auftragsverarbeitung dahingegen als Voraussetzung verlangt, dass eine „rechtliche Einheit" zwischen Auftraggeber und Auftragnehmer vorliegt, so dass der Auftragnehmer **nicht** als „Dritter" zu betrachten ist, der eigenständig und außerhalb des Einflussbereichs des Auftraggebers agiert. Diese Einheit wurde grundsätzlich verneint, wenn der Auftragnehmer seinen Sitz im EU-Ausland hat. Damit – so die Rechtsauffassung – war der Auftragnehmer stets Dritter und der Abschluss

eines Vertrags zur Auftragsverarbeitung ausgeschlossen. Dies hat sich nun geändert. Allerdings verlangen die unabhängigen Aufsichtsbehörden des Bundes und der Länder weiterhin, dass in dem Drittstaat ein angemessenes Schutzniveau bestehen muss. Nach der Datenschutzgrundverordnung müssen die zusätzlichen Anforderungen der Artikel 44 ff. DSGVO für Verarbeitungen in Drittstaaten eingehalten werden (geeignete Garantien nach Artikel 46 DSGVO wie z.B. Standarddatenschutzklauseln).

Sofern rechtswidrig auf einen Vertrag zur Auftragsverarbeitung verzichtet wird, droht ein Bußgeld bis zu 10 Millionen Euro oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (Artikel 83 Absatz 4a) i.V.m. Artikel 28 DSGVO).
(https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf).

B. Einzelne Rechtsfragen

Insgesamt bedürfen einzelne Rechtsfragen in der Praxis besonderer Aufmerksamkeit, etwa die Abgrenzung zur Funktionsübertragung oder die Anwendung auf Fernwartungsverträge.

Die Datenschutzkonferenz vertritt die Auffassung, dass IT-Wartungsverträge den Anforderungen des Artikel 28 DSGVO genügen müssen (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf). Für andere Dienstleistungen ist hingegen gemäß der Auffassung der Aufsichtsbehörde kein Vertrag zur Auftragsverarbeitung erforderlich. Umfasst sind davon unter anderem die Einbeziehung von Berufsgeheimnisträgern (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer), Inkassobüros mit Forderungsübertragung, Bankinstitute für den Geldtransfer sowie Postdienste für den Brieftransport. Daher muss bei diesen Fallgestaltungen im Einzelfall und pro jeweiliger Datenverarbeitung geprüft werden, welche Daten für welchen Zweck aufgrund einer Einwilligung des Betroffenen oder berechtigter Interessen oder auch aus dem Grunde verarbeitet werden dürfen, da die Datenverarbeitung für die Vertragserfüllung erforderlich ist. Aufgrund der Rechenschaftspflichten des Verantwortlichen (Artikel 5 Absatz 2 DSGVO) muss dies ebenso dokumentiert werden. Das Bayerische Landesamt für Datenschutzaufsicht führt speziell für Steuerberaterinnen und Steuerberater aus, dass mangels Weisungsgebundenheit keine Auftragsverarbeitung nach Artikel 28 DSGVO vorliegt (https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Steuerberater_keine_ADV.pdf). Bezüglich der Tätigkeit von Ärzten stellt die Bayerische Behörde eine Auslegungshilfe zur Verfügung, unter welchen Voraussetzungen eine Auftragsverarbeitung in Betracht kommen kann. Im Übrigen soll auch das Hosting von rein statischen Websites (zur Selbstdarstellung) z.B. von Vereinen oder Kleinunternehmen, keine Auftragsverarbeitung darstellen, wenn weder personenbezogenen Daten über die Seitenaufrufe an den Verein oder das Kleinunternehmen fließen noch Nutzer-Tracking stattfindet (https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Hosting_keine_Auftragsverarbeitung.pdf dar, dass das Hosting).

Weiterhin muss die Auftragsverarbeitung von den Fallgestaltungen der gemeinsamen Verantwortlichkeit (Artikel 26 DSGVO) abgegrenzt werden. Grundsätzlich bedeutet „gemeinsame Verantwortlichkeit“, dass derjenige, der in der Praxis Einfluss auf die Zwecke und die Mittel der Verarbeitung hat, bei Rechtsverstößen zur Verantwortung gezogen werden kann. Damit können die Betroffenen ihre Rechte gegenüber den Verantwortlichen leichter durchsetzen, und zwar auch in dem Falle, dass mehrere Verantwortliche bei der Datenverarbeitung kooperieren und sich arbeitsteilig zusammenschließen. In der Praxis hat dieses so genannte „Joint Controllership“ vor allem Aufmerksamkeit durch das Urteil des Europäischen Gerichtshofs

erfahren, wonach Betreiber einer Fanpage nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen können, sondern sind selbst mitverantwortlich sind, dass der Datenschutzes gegenüber den Nutzenden ihrer Fanpage eingehalten wird (https://www.datenschutzkonferenz-online.de/media/en/20180605_en_fb_fanpages.pdf).

C. Links und Materialien

Datenschutzkonferenz

Die Datenschutzkonferenz hat eine Orientierungshilfe veröffentlicht, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

Auf S. 3 dieses Kurzpapiers findet sich die oben unter A. dargestellte Auffassung, dass IT-Wartungsverträge den Anforderungen des Artikel 28 DSGVO genügen müssen.

Auf S. 4 sind Beispiele für die Inanspruchnahme fremder Fachleistungen aufgeführt, die keine Auftragsverarbeitung darstellen sollen, sondern deren Rechtmäßigkeit - gemäß der Rechtsauffassung der Datenschutzbehörden - anhand der Rechtsgrundlage des Artikel 6 DSGVO zu bewerten sind. Dies bedeutet, dass für manche Dienstleistungen kein Vertrag zur Auftragsverarbeitung abgeschlossen werden muss. Umfasst sind davon (wie oben unter B. dargestellt) unter anderem die Einbeziehung von Berufsgeheimnisträgern (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer), Inkassobüros mit Forderungsübertragung, Bankinstitute für den Geldtransfer sowie Postdienste für den Brieftransport.

In dem Kurzpapier geht die Datenschutzkonferenz außerdem auf den Punkt der „gemeinsamen Verantwortlichkeit“ näher ein (Artikel 26 DSGVO). Sie betont, dass diese in Abgrenzung zur Auftragsverarbeitung zu sehen sei und verweist auf die alte Rechtslage, unter welcher diese Konstellation teilweise als Funktionsübertragung eingestuft wurde. Als Beispiele für eine gemeinsame Verantwortlichkeit unterschiedlicher Dienstleister werden klinische Arzneimittelstudien oder die gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen genannt. Grundsätzlich wird mit der gemeinsamen Verantwortlichkeit gemäß Artikel 26 DSGVO sichergestellt, dass derjenige, der in der Praxis Einfluss auf die Zwecke und die Mittel der Verarbeitung hat, bei Rechtsverstößen zur Verantwortung gezogen werden kann. In diesem Zusammenhang ist ergänzend auf das Urteil des Europäischen Gerichtshofs hinzuweisen, welches von der Datenschutzkonferenz begrüßt wird. Siehe hierzu Entschließung vom 06.06.2018 - https://www.datenschutzkonferenz-online.de/media/en/20180605_en_fb_fanpages.pdf: „Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt. Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.“

Bayerisches Landesamt für Datenschutzaufsicht

Unter https://www.lda.bayern.de/de/thema_auftragsverarbeitung.html hat die Behörde einige Informationen und Links zum Thema Auftragsverarbeitung zusammengestellt:

Unter https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf ist eine Formulierungshilfe für einen Vertrag zur Auftragsverarbeitung zu finden.

Der folgende Link beinhaltet eine Auslegungshilfe für die Abgrenzung einer Auftragsverarbeitung; https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

Unter https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Auftragsverarbeitung_Arzt.pdf ist eine Auslegungshilfe zur Frage zu finden, ob ein Arzt eine Auftragsverarbeitung vornimmt.

Die Formerfordernisse einer Auftragsverarbeitung werden unter folgendem Link skizziert: https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_ADV_Formerfordernis.pdf.

Die Behörde stellt unter https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Hosting_keine_Auftragsverarbeitung.pdf dar, dass das Hosting von rein statischen Websites (zur Selbstdarstellung) z.B. von Vereinen oder Kleinunternehmen, keine Auftragsverarbeitung ist, wenn keine personenbezogenen Daten über die Seitenaufrufe an den Verein oder das Kleinunternehmen fließen und auch kein Nutzer-Tracking stattfindet.

Aus Sicht der Aufsichtsbehörde stellt außerdem die Tätigkeit von Steuerberaterinnen und Steuerberatern mangels Weisungsgebundenheit keine Auftragsverarbeitung nach Art. 28 DS-GVO dar:https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Steuerberater_keine_ADV.pdf

Die Landesbeauftragte für den Datenschutz Niedersachsen

Die Landesbeauftragte für den Datenschutz Niedersachsen hat ein Vertragsmuster als Formulierungshilfe für die Auftragsverarbeitung zur Verfügung gestellt: https://www.lfd.niedersachsen.de/download/127630/Formulierungshilfe_zur_Auftragsverarbeitung_nach_Art._28_DS-GVO.pdf. Unter https://lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung_nach_art_28_ds_gvo/auftragsverarbeitung-nach-art-28-ds-gvo-179673.html findet sich ein kurzer Überblick. FAQ zur Auftragsverarbeitung sind unter https://lfd.niedersachsen.de/download/156382/FAQ_zur_Auftragsverarbeitung_nach_Art._28_DS-GVO.pdf zu finden.

Der Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Unter folgendem Link wird ein Mustervertrag zur Verfügung gestellt: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/200429_AVV-Muster_DE.pdf

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

In den FAQ sind unter der Rubrik „Was ist neu bei der Auftrags(daten)verarbeitung“ die Neuerungen im Detail aufgelistet: https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/faq/

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Unter https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/Formulierungshilfe%20Auftragsverarbeitungsvertrag/Formulierungshilfe_AVV.docx stellt der Landesbeauftragte eine Formulierungshilfe „Auftragsverarbeitung" zum Download bereit.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

Eine Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach der DSGVO findet sich unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf.

bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)

bitkom hat einen Mustervertrag veröffentlicht, abrufbar unter https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf , und unter https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf begleitende Hinweise erstellt.

In einer Executive Summary (S. 8 ff.) werden zunächst die Änderungen an der Auftragsverarbeitung durch die Datenschutz-Grundverordnung zusammengefasst, z.B. auch die Veränderungen in den Begrifflichkeiten (Auftragsdatenverarbeitung => Auftragsverarbeitung).

Auf S. 17 ff. („Wann liegt eine Auftragsverarbeitung vor?") wird dargestellt, wie eine Datenübermittlung von einer Auftragsverarbeitung abzugrenzen ist und was unter einer gemeinsamen Verantwortlichkeit im Gegensatz zur Auftragsverarbeitung zu verstehen ist. Die Ausführungen auf S. 27 behandeln die wichtigen und notwendigen Dokumentationspflichten des Auftragsverarbeiters gegenüber dem Auftraggeber und der Datenschutzaufsichtsbehörde.

Darüber hinaus stellt die bitkom unter https://www.bitkom.org/sites/default/files/file/import/170515-Joint-Controllership-online.pdf außerdem eine Checkliste zur Prüfung einer gemeinsamen Verantwortlichkeit zur Verfügung („Joint Controllership" – Artikel 26 DSGVO).

GDD (Gesellschaft für Datenschutz und Datensicherheit e.V.)

Der GDD stellt eine Praxishilfe unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf zur Verfügung. Hervorzuheben ist der Verweis auf die IT-Wartung oder Fernwartung (S. 1/2). Der GDD führt aus, dass es sich nach Meinung der hiesigen Aufsichtsbehörden um eine Form der Auftragsverarbeitung handele und die Anforderungen des Artikel 28 DSGVO gelten sollen, wenn der Verantwortliche den Dienstleister mit einer IT-Wartung betraut und dabei die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten des Auftraggebers bestehe. Weiterhin stellt der GDD unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf ein Vertragsmuster und eine Synopse der Verpflichtungen unter BDSG (alt) und DSGVO bereit. Die entsprechenden Musterverträge stellt der GDD in deutscher (https://www.gdd.de/downloads/praxishilfen/ph-iv-musterver-

trag_zur_auftragsverarbeitung_ds-gvo-2) und englischer Sprache (https://www.gdd.de/downloads/praxishilfen/ph-iv-mustervertrag_zur_auftragsverarbeitung_ds-gvo_english) zur Verfügung.

Unter https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/auftragsverarbeitungs-mustervertrag-fuer-das-gesundheitswesen/muster-vertrag-pdf/at_download/file ist außerdem ein kommentierter Vertrag zur Auftragsverarbeitung für das Gesundheitswesen zu finden.

Hinweise zum Umgang mit Altverträgen stellt die GDD unter https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/auftragsverarbeitungs-mustervertrag-fuer-das-gesundheitswesen/umgang-mit-altvertraegen/at_download/file bereit.

Darüber hinaus werden Informationen zur gemeinsamen Verantwortlichkeit („Joint Controllership" – Artikel 26 DSGVO) unter https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_15_JointControllership_1.0.pdf zur Verfügung gestellt.

Zentralverband des Deutschen Handwerks (ZDH)

Speziell für das Handwerk hat der Zentralverband des Deutschen Handwerks e.V. ein Vertragsmuster veröffentlicht: https://www.zdh.de/fileadmin/user_upload/themen/Recht/Datenschutz/Handwerksorganisation/Anlage_1_Musterformulierungen_Auftragsverarbeitung.docx (Muster Auftragsverarbeitung)

Verbände aus dem Gesundheitswesen

Zum Umgang mit Altverträgen sind Hinweise im Rahmen einer Zusammenarbeit zwischen dem Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD), dem Bundesverband Gesundheits-IT e.V. (bvitg), der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (gmds), der Deutschen Krankenhausgesellschaft e.V. ((Deutsche Krankenhausgesellschaft) sowie der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) erarbeitet worden, abrufbar unter https://www.bvdnet.de/wp-content/uploads/2017/07/17_Umgang_Altvertraege.pdf (siehe auch oben unter den Hinweisen der GDD).

IHK Saarland

Die IHK Saarland hat Hinweise zur Auftragsverarbeitung nach der DSGVO veröffentlicht - https://www.saarland.ihk.de/ihk-saarland/Integrale?SID=CRAWLER&MODULE=Frontend.Media&ACTION=ViewMediaObject&Media.PK=7451&Media.Object.ObjectType=full.

IHK Nürnberg

Die IHK Nürnberg hat einen Praxisleitfaden zur Auftragsverarbeitung und Anforderungen an die betriebliche Organisation erstellt, abrufbar unter https://www.ihk-nuernberg.de/de/media/PDF/Innovation-Umwelt/it/datenschutz/praxisleitfaden-auftragsverarbeitung.pdf.

Telemedicus - Dr. Malte Engeler

Ein juristischer Beitrag zur Auftragsverarbeitung ist auf dem Portal Telemedicus (juristisches Non-Profit-Projekt) veröffentlicht, abrufbar unter https://www.telemedicus.info/article/3150-Die-Auftragsdatenverarbeitung-braucht-ein-Reboot-mit-der-DSGVO-in-der-Hauptrolle.html.

Europaweite Links:

EU-Kommission

Definitionen zu den Begriffen der Auftragsverarbeitung, des Verantwortlichen und des Auftragsverarbeiter sind auf der Webseite der EU-Kommission zu finden: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor_de.

ICO: Britische Datenschutzbehörde (Information Commissioner's Office) :

Eine englischsprachige Checkliste und Handlungsempfehlung hinsichtlich der Pflichten von Auftragsverarbeiter und Verantwortlichem stellt die britische Datenschutzbehörde (ICO) zur Verfügung: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf.

Isle of Man Information Commissioner (Datenschutzbehörde Isle of Man):

Unter https://www.inforights.im/organisations/data-protection-law-2018/controllers-and-processors/ erörtert die Datenschutzbehörde die Verpflichtungen von Auftragsverarbeitern und stellt weiterführende Links bereit.

CNIL (Datenschutzbehörde Frankreich)

Die CNIL hat unter https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf Empfehlungen für Auftragsverarbeiter veröffentlicht.

CNPD (Datenschutzbehörde Luxemburg)

Eine Präsentation über „Verpflichtungen von Verantwortlichen und Auftragsverarbeitern“ ist auf der Webseite der Datenschutzbehörde von Luxemburg abrufbar - https://cnpd.public.lu/content/dam/cnpd/fr/actualites/national/2018/formation-cnpd-intro-pd/en-3-obligations-dur.pdf.