DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

Dossier VI: Auftragsverarbeitung

Stand: August 2018

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- ebenso 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, dass die Datenschutzgrundverordnung dem Auftragsverarbeiter mehr Rechtspflichten auferlegt (z.B. Verzeichnis für Verarbeitungstätigkeiten) und zudem Haftungsregelungen bei Datenschutzverletzungen enthält.

Außerdem kann nun 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. 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).

Insgesamt sind jedoch einzelne Rechtsfragen ungeklärt, 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.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf).

B. Links und Materialien

- **Datenschutzkonferenz**

  Die Datenschutzkonferenz hat eine Orientierungshilfe veröffentlicht, abrufbar unter https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

  Hier findet sich auf S. 3 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 anhand der Rechtsgrundlage des Artikel 6 DSGVO zu bewerten sei. Dies umfasst unter anderem die Einbeziehung von Berufsgeheimnisträgern (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer), Inkassobüros mit Forderungsübertragung, Bankinstitute für den Geldtransfer sowie Postdienste für den Brieftransport.

  Weiterhin wird seitens der Datenschutzkonferenz auf die Möglichkeit der gemeinsamen Verantwortlichkeit eingegangen, die in Abgrenzung zur Auftragsverarbeitung zu sehen sei und unter den Regelungen des Bundesdatenschutzgesetzes teilweise als Funktionsübertragung eingestuft wurde. Als Beispiele werden klinische Arzneimittelstudien oder die gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen genannt.

  In diesem Zusammenhang und in Bezug auf eine gemeinsame datenschutzrechtliche Verantwortung ist ergänzend auf das Urteil des Europäischen Gerichtshofs hinzuweisen. Dieses Urteil wird von der Datenschutzkonferenz begrüßt. 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.“*

- **Landesbeauftragte für den Datenschutz Niedersachsen:**

  Auch 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://www.lfd.niedersachsen.de/themen/auftragsdatenverarbeitung/auftragsverarbeitung-nach-art-28-ds-gvo-161994.html findet sich ein kurzer Überblick.

- **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-grundverordung/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.

- **Bayerisches Landesamt für Datenschutzaufsicht**
  https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf (Kurzpapier Auftragsverarbeitung)
  https://www.lda.bayern.de/media/muster_adv.pdf (Formulierungshilfe Auftragsverarbeitung)

- **Artikel-29-Datenschutzgruppe**
  Die Artikel-29-Datenschutzgruppe hat Empfehlungen zur „Auftragsdatenverarbeitung“ veröffentlicht, allerdings noch unter der Richtlinie 95/46/EG - http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

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

  Die 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. 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.

- **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.

- **Zentralverband des Deutschen Handwerks (ZDH)**

  Speziell für das Handwerk hat der Zentralverband des Deutschen Handwerks e.V. ein Vertragsmuster veröffentlicht.
  http://www.hwk-aachen.de/fileadmin/user_upload/downloads/eu-datenschutzgrundverordnung/ZDH_Praxis_Datenschutz_Auftragsverarbeitung_Handwerksbetriebe.pdf und https://www.zdh.de/fachbereiche/organisation-und-recht/datenschutz/datenschutz-fuer-handwerksorganisationen/ (allgemeine Hinweise)

  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 http://ds-gvo.gesundheitsdatenschutz.org/download/Umgang_Altvertraege.pdf

- **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/Datenschutz-in-der-betrieblichen-Praxis/praxisleitfaden-auftragsverarbeitung.pdf.

- **Telemedicus - *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/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-depth/processors-the-new-obligations/ erörtert die Datenschutzbehörde die Verpflichtungen von Auftragsverarbeitern.

- **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-du-rt.pdf