DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

DIE DATENSCHUTZGRUNDVERORDNUNG

Juni 2020

Prof. Dr. Anne Riechert

In diesem Dossier erfolgt ein Überblick zum Datenschutzrecht und Regelungen der DSGVO:

A. Aufsichtsbehörden, Sanktionen und Meldepflichten

B. Dokumentationspflichten und Verzeichnis von Verarbeitungstätigkeiten

C. Datenschutz-Folgenabschätzung

D. Datenschutzbeauftragte

E. Auftragsverarbeitung

F. Übermittlung personenbezogener Daten an Drittländer

G. Transparenz der Datenverarbeitung

H. Werbung

Nähere Details und weiterführende Materialien zu den nachfolgend aufgelisteten Themenbereichen können den einzelnen Dossiers entnommen werden, die ebenfalls auf der Webseite der Stiftung Datenschutz abrufbar sind:

A. Aufsichtsbehörden, Sanktionen und Meldepflichten

Die Aufsichtsbehörden können Geldbußen verhängen, die gemäß der Intention der Datenschutzgrundverordnung in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein sollen. Die Sanktionen des Artikels 83 DSGVO sehen bei schwerwiegenden Verstößen Geldbußen bis 20 Millionen EURO oder 4% des weltweiten Gesamtumsatzes des vergangenen Geschäftsjahres vor. Allerdings ist zu berücksichtigen, dass die Verhängung einer Geldbuße nur eine Sanktionsmöglichkeit darstellt. So können Aufsichtsbehörden außerdem vorsorgliche Warnungen oder im Falle von Datenschutzverletzungen Verwarnungen (Artikel 58 DSGVO) aussprechen. Bei Nichtbefolgung ihrer Anordnungen können sie Zwangsgelder verhängen. Auf europäischer Ebene wurde das noch unter der Artikel-29-Datenschutzgruppe erarbeitete WP 253 „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verord-

Stand: Juni 2020

Autorin: Prof. Dr. Anne Riechert

nung (EU) 2016/679“ vom Europäischen Datenschutzausschuss angenommen: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 und https://www.lda.brandenburg.de/media_fast/4055/wp253_de.pdf (deutsch).

In Deutschland hat die Datenschutzkonferenz, das Gremium der unabhängigen deutschen Aufsichtsbehörden des Bundes und der Länder, ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen entwickelt (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeld-konzept.pdf). Es soll keine Anwendung auf Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit finden. Nach diesem Konzept erfolgt die Bußgeldzumessung in fünf Schritten: „*Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.)*.“

Die Datenschutzkonferenz verweist allerdings darauf, dass diese Leitlinien nicht erschöpfend sind und die Konkretisierung der Festsetzungsmethodik den späteren Leitlinien des Europäischen Datenschutzausschusses vorbehalten bleibt.

Ergänzend soll darauf hingewiesen werden, dass das BDSG-alt die Meldepflichten bei Datenschutzverletzungen auf Fälle der unberechtigten Übermittlung von sensiblen Daten oder Kontodaten an Dritte begrenzte. Zudem musste eine schwerwiegende Verletzung des Persönlichkeitsrechts vorliegen. Nach der Datenschutzgrundverordnung (Artikel 33 DSGVO) besteht nun immer, d.h. bei jeder Datenschutzverletzung, eine unverzügliche Meldepflicht (binnen höchstens 72 Stunden) an die zuständige Aufsichtsbehörde, es sei denn der Verantwortliche kann nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Ob ein solches Risiko vorliegt, kann zu Untersicherheiten bei den Unternehmen führen. Als Hilfestellung hat die Datenschutzkonferenz ein entsprechendes Kurzpapier zur Einschätzung eines Risikos für die Rechte und Freiheiten natürlicher Personen veröffentlicht (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben außerdem in ihrem Erfahrungsbericht zur Anwendung der DSGVO darauf hingewiesen, dass die Meldepflicht auf Fälle beschränkt werden sollte, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen (siehe hierzu unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf).

In Kürze:

Die Meldepflicht im Zusammenhang mit Datenpannen ist unter der DSGVO verschärft worden.

Zu berücksichtigen ist jedoch, dass die Verhängung einer Geldbuße lediglich eine (!) Sanktionsmöglichkeit durch die Aufsichtsbehörden darstellt. Möglich ist ebenso, vorsorgliche Warnungen oder im Falle

von Datenschutzverletzungen Verwarnungen auszusprechen.

B. Dokumentationspflichten und Verzeichnis von Verarbeitungstätigkeiten

Unter der Datenschutzgrundverordnung sind zahlreiche Regelungen zu finden, die den Nachweis dafür verlangen, dass die Verarbeitung nach den Regeln der DSGVO erfolgt. Allgemeine Regelungen wie Artikel 5 Absatz 2 DSGVO nehmen auf die sogenannte „Rechenschaftspflicht" Bezug, nach welcher der Verantwortliche einen Nachweis für die Rechtmäßigkeit der Datenverarbeitung erbringen muss. Entsprechendes ist ebenso in Artikel 24 Absatz 1 DSGVO geregelt. Danach muss der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzen, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Daneben sind in Regelungen zu speziellen Bereichen (z.B. Einwilligung, Datenschutz-Folgenabschätzung, Verzeichnis von Verarbeitungstätigkeiten) gleichermaßen Nachweis- und Dokumentationspflichten zu finden.

Das Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO) hat das Verfahrensverzeichnis des BDSG-alt abgelöst. Nunmehr handelt es sich aber im Gegensatz zur alten Regelung um eine interne Dokumentation, die vom Verantwortlichen zu erstellen und auf Anforderung der zuständigen Aufsichtsbehörde vorzulegen ist. Zuvor handelte es sich um öffentliches Verzeichnis, in welches jedermann Einsichtsrechte hatte. Auch Auftragsverarbeiter müssen ein solches Verzeichnis erstellen. Trotz des Bezugs auf eine Unternehmensgröße von mindestens 250 Mitarbeitern muss jedes Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten führen, sofern dort regelmäßig Daten verarbeitet werden. Dies wird den Regelfall darstellen, da die Verarbeitung in den meisten Fällen nicht nur gelegentlich erfolgt. Dies ist den von der Datenschutzkonferenz erstellten Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten zu entnehmen (https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf). Diese enthalten unter anderem Erläuterungen zum Zweck und zur Form des Verzeichnisses. So wird darauf verwiesen, dass die in Artikel 30 DSGVO genannten Ausnahmen nur selten greifen werden. Insbesondere wegen der regelmäßig erfolgenden Lohnabrechnungen werde daher kaum Unternehmen von der Pflicht eines solchen Verzeichnisses generell befreit sein, allenfalls Unternehmen, die diese Tätigkeiten komplett durcheinen Steuerberater erledigen lassen würden sowie eventuell kleinere Vereine. Zudem erfolgt in dem Dokument der Hinweis, dass bei Lohnabrechnungen oder in der Schülerverwaltung mit der Angabe der Konfessionszugehörigkeit zumeist auch gleich besondere Datenkategorien i.S.d. Art. 9 Abs. 1 DS-GVO vorliegen würden.

Zur Gewährleistung eines effektiven Datenschutz-Managementsystems und zu Dokumentationszwecken sollte nach Auffassung der Landesdatenschutzbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zudem in jedem Fall ein schriftliches, internes Verzeichnis von Verarbeitungstätigkeiten erstellt werden, auch wenn dies an sich nicht erforderlich wäre (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Antworten-auf-haeufig-gestellte-Fragen-zu-Datenschutzbeauftragten/Inhalt/III__Aufgaben_der_Datenschutzbeauftragen__Artikel_39_DS-

GVO_Artikel_34_JI-RL/Welche_Rolle_haben_Datenschutzbeauftragte_beim_Verarbeitungsverzeichnis_.php). Hintergrund ist, dass ein Unternehmen stets die Rechtmäßigkeit der Datenverarbeitung nachweisen können muss (Artikel 5 Absatz 2 DSGVO) und sich daher die Erstellung und Vorhaltung zusätzlicher weiterer Dokumentation empfehlen kann. Diese kann auch außerhalb des Verzeichnisses von Verarbeitungstätigkeiten geführt werden und im Verzeichnis eine entsprechende Referenz auf diese Dokumentation erfolgen.

In Kürze:

Die DSGVO verlangt umfassende Dokumentationspflichten, um die Vereinbarkeit der Datenverarbeitung mit den Grundsätzen der Datenschutzgrundverordnung nachzuweisen.

Auch das Verzeichnis von Verarbeitungstätigkeiten erfordert eine solche Dokumentation. Das Verzeichnis ist schriftlich zu führen, wovon ebenso ein elektronisches Format umfasst ist.

Ein Verzeichnis von Verarbeitungstätigkeiten ist praktisch von jedem Unternehmen zu führen, es sei denn, es liegt die Ausnahme der „gelegentlichen" Datenverarbeitung vor.

Das Verzeichnis von Verarbeitungstätigkeiten ist auf Anforderung der zuständigen Aufsichtsbehörde vorzulegen.

C. Datenschutz-Folgenabschätzung

Unter der DSGVO gibt es das Instrument der Datenschutz-Folgenabschätzung (Artikel 35 DSGVO), welches die Vorabkontrolle nach BDSG-alt ablöst. Entsprechend der Vorabkontrolle muss auch unter der DSGVO eine Prüfung dahingehend durchgeführt werden, ob die Verarbeitung *voraussichtlich ein hohes Risiko* für die betroffenen Personen zur Folge hat (insbesondere bei der Verwendung neuer Technologien).

Das „Risiko für die Rechte und Freiheiten natürlicher Personen" stellt insgesamt einen zentralen Begriff in der DSGVO dar und beinhaltet einen risikobasierten Ansatz, der innerhalb der Verordnung an unterschiedlichen Stellen zu finden ist (so z.B. bei Privacy by Design und bei der Sicherheit der Datenverarbeitung, deren Umsetzung sich jeweils an den Rechten und Freiheiten natürlicher Personen orientiert). Kritisiert wird oftmals, dass mangels Definition unklar sei, wann ein „hohes Risiko" für die Rechte und Freiheiten natürlicher Personen besteht. Insgesamt handelt es sich jedoch um einen bekannten Begriff aus der Datenschutzrichtlinie 95/46/EG, der bereits Prüfbestandteil der Vorabkontrolle nach BDSG-alt war. Zu beachten ist nun jedoch, dass die Prüfung im europäischen Kontext vorgenommen werden muss. Daher sind gleichermaßen die Regelungen der Europäischen Menschenrechtskonvention mit einzubeziehen und insgesamt alle Grundrechte, die durch das Datenschutzrecht mittelbar geschützt werden.

Die Datenschutzkonferenz hat außerdem ein Kurzpapier veröffentlicht, dem zu entnehmen ist, unter welchen Voraussetzungen ein solches Risiko vorliegen kann (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). So wird etwa dargestellt, dass die negativen Folgen der ge-

planten Verarbeitung selbst betrachtet werden müssen. Dazu gehören auch Einschränkungen von Rechten und Freiheiten, beispielsweise wenn betroffene Personen aus Angst vor Nachteilen auf die Ausübung ihrer Rechte verzichten (z.B. Verzicht auf Teilnahme an einer Demonstration aufgrund umfangreicher Überwachung).

Zudem sieht die DSGVO die Veröffentlichung von Listen durch die Aufsichtsbehörden vor, in welchen Beispiele für die Durchführung einer Datenschutz-Folgenabschätzung zu finden sind. Die weiterführenden Links zu diesen Listen sind im Dossier Datenschutz-Folgenabschätzung aufgelistet.

In Kürze:

Die Datenschutz-Folgenabschätzung löst die Vorabkontrolle ab.

Es muss eine objektive Ermittlung und Beurteilung des Risikos einer Verarbeitung personenbezogener Daten vorgenommen werden, um festzustellen, wie die Rechte und Freiheiten natürlicher Personen wirksam geschützt werden können. Dabei müssen alle denkbaren negativen Folgen der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, ihre wirtschaftlichen, finanziellen und immateriellen Interessen, ihren Zugang zu Gütern oder Dienstleistungen, für ihr berufliches und gesellschaftliches Ansehen, für ihren gesundheitlichen Zustand und für alle ihre sonstigen legitimen Interessen betrachtet werden (Kurzpapier Datenschutzkonferenz – Rechte und Freiheiten https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). Die Aufsichtsbehörden haben zu diesem Zweck eine Liste der Verarbeitungsvorgänge veröffentlicht, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 35 Absatz 4): https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf. Die Schutzmaßnahmen müssen nachgewiesen werden. Im Rahmen der Vorabkontrolle nach BDSG-alt wurde zwar auch bereits die Auffassung vertreten, dass für die Erfüllung einer ordnungsgemäßen Organisation im Sinne von § 9 BDSG-alt (technische und organisatorische Maßnahmen) eine schriftliche Dokumentation zwingend erforderlich sei. Nunmehr ist eine solche ausführliche Dokumentation jedoch in der DSGVO ausdrücklich verankert.

Gelangt der Verantwortlich zu dem Ergebnis, dass kein Risiko für die Rechte und Freiheiten der betroffenen Personen vorliegt, muss er auch dies dokumentieren („Schwellenwertanalyse“).

D. Der Datenschutzbeauftragte

Die Öffnungsklausel des Artikels 37 Absatz 4 DSGVO sieht vor, dass Verantwortliche einen Datenschutzbeauftragten auf freiwilliger Basis benennen können. Hiervon hat der Bundesgesetzgeber Gebrauch gemacht und die Regelung des § 4f BDSG-alt aufrechterhalten. Gemäß § 38 BDSG-neu besteht dementsprechend weiterhin eine Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten, wenn mindestens 20 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind. Diese Änderung ist am 26.11.2019 in Kraft getreten und hat die Anzahl der Personen, ab der eine Bestellungspflicht besteht, von zehn auf 20 erhöht.

Ein Datenschutzbeauftragter muss außerdem gemäß den Regelungen der **DSGVO** unabhängig von der Anzahl der Personen, die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, stets benannt werden, wenn die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von Personen erfordert *oder* sensible Daten (u.a. Gesundheitsdaten) verarbeitet werden:

Umfangreiche Verarbeitung sensibler Daten

Als Beispiele für eine Bestellpflicht nach Artikel 37 Abs. 1c DSGVO werden Gesundheitseinrichtungen, wie z.B. Krankenhäuser, mit genetischen Untersuchungen befasste Labors, Beratungsstellen wie Pro Familia, Dienstleister im biometrischen ID-Management oder Anbieter von Erotikartikeln genannt (siehe GDD - Gesellschaft für Datenschutz und Datensicherheit -https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0). Für Praxen, die ein einzelner Arzt betreibt, soll nach Auffassung von deutschen Aufsichtsbehörden diese Verpflichtung regelmäßig entfallen, so dass die Grenze des BDSG gilt (Entschließung der Datenschutzkonferenz vom 26.04.2018 -https://www.datenschutzkonferenz-online.de/media/en/20180426_en_dsb_bestellpflicht.pdf). Für Praxen, die ein einzelner Arzt betreibt, soll die verpflichtende Benennung eines Datenschutzbeauftragten mangels umfangreicher Verarbeitung von sensiblen Daten regelmäßig entfallen. Nach Auffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) soll auch der Arzt selbst zu den Personen zählen, die bei der Prüfung zu berücksichtigen sind (https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html). Das ULD legt allerdings noch die alte (bis 25.11.2019 geltende) Gesetzeslage zugrunde, als eine Bestellpflicht für Datenschutzbeauftragte gemäß Bundesdatenschutzgesetz (BDSG) noch bei zehn Personen galt (die mit der Datenverarbeitung beschäftigt sind)().

Kerntätigkeit:

Beispiele für eine Bestellpflicht nach Artikel 37 Abs. 1b DSGVO sind den Ausführungen des GDD zu entnehmen. Danach fallen unter den Begriff einer Kerntätigkeit etwa Auskunfteien, Detekteien, Versicherungsunternehmen (Risikomanagement oder individualisierte Tarife wie „Pay as you drive"), Marketing auf Basis detaillierter Kunden- und Interessentenprofile. Es soll dabei stets darauf ankommen, ob der Geschäftszweck unmittelbar gefördert wird (siehe GDD - Gesellschaft für Datenschutz und Datensicherheit - https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0 ´).

Insoweit kann eine Überschneidung zur **Datenschutz-Folgenabschätzung** vorliegen, da die Anforderungen nach **BDSG-neu** eine Bestellpflicht eines Datenschutzbeauftragten – unabhängig von der Personenanzahl - bei Verarbeitungen vorsehen, die einer Datenschutz-Folgenabschätzung unterliegen. Diese Datenschutz-Folgenabschätzung stellt grundsätzlich kein neues Instrument dar, da diese die Vorabkontrolle nach BDSG-alt ablöst. Allerdings muss nun der Datenschutzbeauftragte diese Prüfung nicht mehr selbst durchführen, sondern sie ist Aufgabe des Verantwortlichen bzw. des verantwortlichen Unternehmens. Dem Datenschutzbeauftragten obliegt lediglich eine Überwachungs- und Beratungsaufgabe. Weitere Details sind dem Punkt „*Datenschutz-Folgenabschätzung*" sowie dem Dossier Datenschutz-Folgenabschätzung zu entnehmen.

Im Gegensatz zur alten Fassung des BDSG wird nun außerdem ausdrücklich die Möglichkeit eines Konzerndatenschutzbeauftragten genannt: Eine Unternehmensgruppe kann einen gemeinsamen Datenschutzbeauftragten benennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht

erreicht werden kann. Eine „Unternehmensgruppe“ wird dabei als Gruppe definiert, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

Zu beachten ist, dass keine gesetzliche Regelung dahingehend vorhanden ist, ob ein Datenschutzbeauftragter eine natürliche Person sein muss. Im Gegensatz zur Meinung des Europäischen Datenschutzausschusses vertritt die-Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Auffassung, dass nur eine natürliche Person (keine juristische Person) als Datenschutzbeauftragter benannt werden sollte (siehe S. 15 unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Antworten-auf-haeufig-gestellte-Fragen-zu-Datenschutzbeauftragten/Inhalt/FAQ_zum_Datenschutzbeauftragten/FAQ_ein_Dokument.pdf). ().

Die Änderung des Wortlauts von „Hinwirken auf die Einhaltung des Datenschutzes“ zu „Überwachung“ soll nach Auffassung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zudem keine persönliche Verantwortung des Datenschutzbeauftragten für die (Nicht-) Einhaltung der rechtlichen Vorgaben beinhalten (siehe S. 29 unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Antworten-auf-haeufig-gestellte-Fragen-zu-Datenschutzbeauftragten/Inhalt/FAQ_zum_Datenschutzbeauftragten/FAQ_ein_Dokument.pdf)). Eine Dokumentation der Beratung empfiehlt sich dennoch für den Datenschutzbeauftragten, da die Grundsätze der Arbeitnehmerhaftung weiterhin Anwendung finden können.

In Kürze:

Die Kontaktdaten des Datenschutzbeauftragten müssen der betroffenen Person bei Erhebung ihrer Daten mitgeteilt werden. Ebenso müssen die Kontaktdaten der zuständigen Aufsichtsbehörde mitgeteilt werden. Die Aufsichtsbehörden stellen zu diesem Zweck Online-Meldeverfahren zur Verfügung.

Nach BDSG ist ein Datenschutzbeauftragter zu benennen, wenn mindestens 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind. Ein Datenschutzbeauftragter muss jedoch gemäß den Regelungen der DSGVO unabhängig von der Anzahl der Personen, die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, stets benannt werden, wenn:

- die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von Personen erfordert

oder

- sensible Daten verarbeitet werden (u.a. Gesundheitsdaten)

Für Praxen, die ein einzelner Arzt betreibt, soll nach Auffassung von deutschen Aufsichtsbehörden diese Verpflichtung allerdings mangels einer umfangreichen Datenverarbeitung regelmäßig entfallen..

E. Auftragsverarbeitung

Das Instrument der Auftragsverarbeitung (Artikel 28 DSGVO) ist 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. Unter dem BDSG-alt wurde der Begriff „Auftrags*daten*verarbeitung“ verwendet. Nunmehr ist die begriffliche Definition „Auftragsverarbeitung“, meint jedoch nach wie vor, dass der Auftragsverarbeiter bei der Auftragsverarbeitung personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet und weisungsgebunden ist.

Insgesamt werden Auftragsverarbeiter nach der DSGVO allerdings stärker in die Pflicht genommen und können eigenen Haftungsansprüchen ausgesetzt sein. Außerdem kann nun auch mit einem Dienstleister, der seinen Geschäftssitz außerhalb der Europäischen Union hat, ein Vertrag zur Auftragsverarbeitung geschlossen werden. Unter altem Recht wurde dies seitens der Aufsichtsbehörden abgelehnt, da in einem solchen Fall der Auftragnehmer stets als Dritter eingeordnet wurde, so dass keine Auftragsdatenverarbeitung 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 bzw. dass die zusätzlichen Anforderungen der Artikel 44 ff. DSGVO für Verarbeitungen in Drittstaaten eingehalten werden (geeignete Garantien nach Artikel 46 DSGVO wie z.B. Standarddatenschutzklauseln).

Die Auftragsverarbeitung muss außerdem 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. Relevanz hat dies etwa für Betreiber einer Website, in der der „Gefällt mir“-Button von Facebook eingebunden ist. Gemäß einer Entscheidung des Europäischen Gerichtshofs vom 29.07.2019 kann dieser für das Erheben und die Übermittlung der personenbezogenen Daten der Besucher seiner Website gemeinsam mit Facebook verantwortlich sein (siehe die Pressemitteilung, abrufbar unter https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099de.pdf).

In Kürze:

Im Rahmen der DSGVO gibt es nach wie vor die Möglichkeit, dass Daten von Dienstleistern im Auftrag eines Verantwortlichen verarbeitet werden. Anders als im BDSG-alt wird nun jedoch der Begriff „Auftragsverarbeitung“ verwendet.

Die DSGVO legt den Auftragsverarbeitern mehr Rechtspflichten auf, so unter anderem das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten, und enthält außerdem eigene Haftungsregelungen bei Datenschutzverletzungen.

Die Auftragsverarbeitung muss vom so genannten „Joint Controllership“ (gemeinsame Verantwortung) unterschieden werden.

Stand: Juni 2020

Autorin: Prof. Dr. Anne Riechert

F. Übermittlung personenbezogener Daten an Drittländer

Werden personenbezogene Daten in Länder außerhalb der EU/EWR (so genannte Drittländer/Drittstaaten) übermittelt, muss dort ein Datenschutzniveau vorliegen, das dem in der Datenschutzgrundverordnung gewährleisteten Schutz gleichwertig ist. Rechtsgrundlage sind Artikel 44 bis Artikel 49 DSGVO.

Das angemessene Datenschutzniveau kann entweder durch einen Angemessenheitsbeschluss der EU-Kommission festgestellt werden oder es müssen geeignete Garantien vorliegen. Der Angemessenheitsbeschluss der Europäischen Kommission im Hinblick auf Unternehmen mit Sitz in den USA galt in der Vergangenheit einschränkend für die Unternehmen, die sich verpflichtet haben, den Datenschutzstandard des EU-US Privacy Shield einzuhalten. Aufgrund einer Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 wurde das Privacy Shield allerdings für ungültig erklärt, so dass auf dieser Grundlage keine personenbezogenen Daten in die USA übermittelt werden dürfen (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Im Hinblick auf die geeigneten Garantien, die ebenfalls ein angemessenes Datenschutzniveau sicherstellen können, wurden die Instrumente der genehmigten Verhaltensregeln und des genehmigten Zertifizierungsmechanismus neu eingeführt, um die Verarbeitung von Daten in Drittstaaten zu legitimieren. Darin müssen rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters festgelegt werden, die außerdem seitens der zuständigen Aufsichtsbehörde zu genehmigen sind. Die praktische Relevanz dieser beiden Instrumentarien bleibt abzuwarten.

Im Rahmen der geeigneten Garantien verwendet die Datenschutzgrundverordnung darüber hinaus nicht mehr den Begriff der „EU-Standardvertragsklauseln“ sondern „Standarddatenschutzklauseln“. Standarddatenschutzklauseln dürfen ohne vorherige Zustimmung der zuständigen Datenschutz-Aufsichtsbehörden verwendet werden. Aufsichtsbehörden können ebenso eigene Standarddatenschutzklauseln veröffentlichen. Die Europäische Kommission hat in der Vergangenheit EU-Standardvertragsklauseln zur Sicherstellung eines angemessenen Datenschutzniveaus unter der Richtlinie 95/46/EG veröffentlicht. Es bleibt abzuwarten, wann diese bisherigen Klauseln durch einen neuen Beschluss der EU-Kommission ersetzt werden. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern sind aufgrund der Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 auch weiterhin gültig (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Sofern weder ein Angemessenheitsbeschluss noch geeignete Garantien vorliegen, ist eine Übermittlung in Drittstaaten möglich, wenn die betroffene Person ausdrücklich eingewilligt hat oder eine Übermittlung in einen Drittstaat aus folgenden Gründen erforderlich ist:

- zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person,
- aus wichtigen Gründen des öffentlichen Interesses (z.B. Steuer- und Zollbehörden),
- zur Verfolgung von Rechtsansprüchen,
- zum Schutz lebenswichtiger Interessen.

Stand: Juni 2020

Autorin: Prof. Dr. Anne Riechert

Der Europäische Datenschutzausschuss vertritt die Auffassung, dass diese Ausnahmen restriktiv auszulegen sind (Leitlinien 2/2018 vom 25.05.2018, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf).

In Kürze:

Übermittelt der Verantwortliche personenbezogene Daten in Länder außerhalb der EU/EWR (Drittländer/Drittstaaten), muss ein Datenschutzniveau vorliegen, das dem in der Datenschutzgrundverordnung gewährleisteten Schutz gleichwertig ist. Als geeignete Garantien wurden die Instrumente der genehmigten Verhaltensregeln und genehmigten Zertifizierungsmechanismen in der Datenschutzgrundverordnung neu verankert. Die Europäische Kommission hat in der Vergangenheit außerdem EU-Standardvertragsklauseln zur Sicherstellung eines angemessenen Datenschutzniveaus veröffentlicht, die vorerst in Kraft bleiben, es sei denn, die EU-Kommission ersetzt diese durch einen neuen Beschluss. Im Übrigen verwendet die Datenschutzgrundverordnung nicht mehr den Begriff der „EU-Standardvertragsklauseln" sondern „Standarddatenschutzklauseln".

Für Datenübermittlungen in die USA ist zu beachten, dass der Europäische Gerichtshof in seiner Entscheidung vom 16.07.2020 das EU-US Privacy Shield für ungültig erklärt hat. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern sind hingegen weiterhin gültig (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Ein Verantwortlicher kann gemäß der Datenschutzgrundverordnung nunmehr außerdem einen Auftragsverarbeitungsvertrag mit einem Dienstleister abschließen, der seinen Geschäftssitz nicht innerhalb der Europäischen Union hat (z.B. Cloudanbieter), sofern dort **zusätzlich** ein **angemessenes Datenschutzniveau** festgestellt werden kann.

Ergänzend:

Die Datenschutzgrundverordnung gilt für alle Datenverarbeitungstätigkeiten, die im Rahmen der Tätigkeiten eines Verantwortlichen oder Auftragsverarbeiters mit Hauptsitz oder Niederlassung in der Europäischen Union erfolgen. Dabei ist unerheblich, an welchem Ort die Datenverarbeitung konkret erfolgt. Die Datenschutzgrundverordnung findet außerdem Anwendung, wenn der Verantwortliche seinen Geschäftssitz *nicht* innerhalb der Europäischen Union hat, er aber personenbezogene Daten im Zusammenhang mit einem Waren- und Dienstleistungsangebot verarbeitet (Artikel 3 DSGVO).

G. Transparenz der Datenverarbeitung

In der DSGVO wird der Transparenzgedanke hervorgehoben und betont, dass die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen (Artikel 5 Absatz 1).

Dementsprechend müssen den betroffenen Personen auch alle Informationen und Mitteilungen zur Geltendmachung ihrer Rechte in präziser, transparenter, verständlicher sowie leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden. Dies muss unentgeltlich erfolgen (Artikel 12 DSGVO).

Explizit werden nun außerdem **Fristen** für die Geltendmachung der Betroffenenrechte genannt. So muss der Verantwortliche vor allem bei den Rechten auf Auskunft (Artikel 15 DSGVO), Berichtigung (Artikel 17 DSGVO) oder Löschung (Artikel 18 DSGVO) sowie beim Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) auf jeden Antrag des Betroffenen fristgebunden reagieren.

Hervorzuheben ist, dass umfassende **Informationspflichten** (Artikel 13 und Artikel 14 DSGVO) aufgezählt sind, die der Verantwortliche **zum Zeitpunkt der Erhebung** der Daten erfüllen muss. Werden Daten über die betroffene Person bei Dritten erhoben (Artikel 14 DSGVO), muss der Verantwortliche zusätzlich über die Datenquelle sowie über die Kategorien der verarbeitenden personenbezogenen Daten informieren. In diesem Falle müssen die Informationen außerdem nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten der betroffenen Person mitgeteilt werden - längstens innerhalb eines Monats.

Insgesamt beinhalten die Regelungen des Artikel 13 DSGVO und Artikel 14 DSGVO in ihrem jeweiligen Absatz 2 zusätzliche Informationspflichten, die zum Zeitpunkt der Datenerhebung zu erfüllen sind und die *notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten*. In diesem Zusammenhang ist auf die Auffassung des Europäischen Datenschutzausschusses zu verweisen, der keinen Unterschied zwischen den Informationspflichten des Absatz 1 und Absatz 2 macht (siehe Leitlinien der der Artikel-29-Datenschutzgruppe,WP 260, S. 12 (abrufbar unter https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025), die vom Europäischen Datenschutzausschuss bestätigt wurden (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de). Daher empfiehlt sich für Unternehmen, umfassend über die Datenverarbeitung anhand der Kriterien der Absätze 1 und 2 zu informieren. Anderenfalls müsste im Einzelfall nachweisbar sein, aus welchem Grunde eine Information nach Absatz 2 nicht erforderlich ist.

Hinsichtlich des **Auskunftsrechts** (Artikel 15 DSGVO) muss der Verantwortliche dem Betroffenen eine elektronische Kopie der Daten zur Verfügung stellen, wenn dieser einen elektronischen Antrag stellt. Dies kann etwa in Form eines pdf-Dokuments erfolgen. Insgesamt kann die Auskunft schriftlich, elektronisch, mündlich oder per Fernzugriff (zu einem sicheren System) erfolgen. Bei mündlichen Auskunftsanfragen bestehen jedoch erhöhte Anforderungen an die Identitätsfeststellung. In der Praxis unterliegt der Umfang des Auskunftsrechts derzeit einer Einzelfallprüfung. So ist unklar, ob eine Kopie aller verfügbaren verarbeiteten personenbezogenen Daten, inklusive des gesamten E-Mailverkehrs, verlangt werden kann. Diese Frage wird von der Rechtsprechung uneinheitlich bewertet. Details können den Handreichungen →*Informationspflichten* bzw. →*Auskunftsrechte* entnommen werden.

Stand: Juni 2020

Autorin: Prof. Dr. Anne Riechert

In Kürze:

Die DSGVO betont die Transparenz der Datenverarbeitung und es muss sichergestellt sein, dass die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Dementsprechend gibt es „ein Mehr" an Informationspflichten, die seitens des Verantwortlichen gegenüber der betroffenen Person erfüllt werden müssen.

Die DSGVO sieht für die Erfüllung sämtlicher Betroffenenrechte, die mittels Antrag geltend gemacht werden, eine Frist von einem Monat vor, die nur in begründeten Ausnahmefällen um weitere zwei Monate verlängert werden darf (Artikel 12 Absatz 3 DSGVO).

In Bezug auf das **Auskunftsrecht** ist nun explizit ein Anspruch auf Erhalt einer elektronischen Kopie vorgesehen.

Ergänzend:

Das Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) stellt ein neues Recht dar, welches im BDSG-alt oder in der Richtlinie 95/46/EG nicht vorgesehen war. Näheres kann der Studie der Stiftung Datenschutz „Praktische Umsetzung des Rechts auf Datenübertragbarkeit" entnommen werden, die auf der Webseite der Stiftung abrufbar ist.

Das Recht auf Löschung („Recht auf Vergessenwerden") gemäß Artikel 17 DSGVO war in dieser Ausgestaltung ebenfalls nicht im BDSG-alt verankert. Es stellt jedoch eine Umsetzung des Urteils des Europäischen Gerichtshofs dar (Google-Spain , Urteil vom 13.05.2014, Az. C-131/12 - http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=DE), indem in Artikel 17 Absatz 2 DSGVO ein erweiterter Löschungsanspruch normiert wurde.

H. Werbung

Werbemaßnahmen können mit einem „berechtigten Interesse" (Artikel 6 Absatz 1f DSGVO) des Verantwortlichen begründet werden. Gemäß Erwägungsgrund 47 der DSGVO kann die Direktwerbung ein solches berechtigtes Interesse des Verantwortlichen grundsätzlich darstellen. Eine Hilfestellung bietet die Orientierungshilfe für Zwecke der Direktwerbung, die die Datenschutzkonferenz veröffentlicht hat (https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf).

Bei der Interessenabwägung im Rahmen von Artikel 6 Absatz 1f DSGVO spielen die vernünftigen Erwartungen der betroffenen Personen eine große Rolle, die im Wesentlichen durch die Informationen (Artikel 13, 14 DSGVO) bestimmt werden. Dabei kann auch zu berücksichtigen sein, ob bereits eine Geschäftsbeziehung zwischen den Beteiligten besteht („ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt" - siehe hierzu das Kurzpapier Werbung der Datenschutzkonferenz (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf).

Nach der Datenschutzgrundverordnung muss außerdem stets ein ausdrücklicher und verständlicher Hinweis auf das jederzeitige Widerspruchsrecht im Rahmen von Werbemaßnahmen erfolgen (Art. 21 DSGVO).

Im Hinblick auf Direktwerbung per E-Mail sind darüber hinaus die Regelungen des UWG (Gesetz gegen den unlauteren Wettbewerb) zu berücksichtigen: Es dürfen ohne Einwilligung des Kunden nur eigene ähnliche Produkte beworben werden, sofern der Verantwortliche dessen E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat und deutlich auf das Widerspruchsrecht hingewiesen wurde (§ 7 Absatz 3 UWG).

Ergänzend und im Rahmen von Online-Werbung soll außerdem die Auffassung der Datenschutzkonferenz besonders erwähnt werden (https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf): Danach bedarf es bei der Erstellung von Nutzerprofilen sowie beim Einsatz von Tracking-Mechanismen einer vorherigen Einwilligung. Dies bedeutet, dass vor der Datenverarbeitung eine informierte Einwilligung i. S. d. DSGVO eingeholt werden muss, beispielsweise bevor Cookies platziert bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden. Diese Auffassung wurde vom Europäischen Gerichtshof in einem Vorabentscheidungsverfahren bekräftigt, welches der Bundesgerichtshof eingeleitet hatte. Gegenstand dieses Verfahrens war die Auslegung des Unionsrechts über den Schutz der Privatsphäre in der elektronischen Kommunikation (siehe Urteil des Europäischen Gerichtshofs vom 01.10.2019 , abrufbar unter http://curia.europa.eu/juris/document/document.jsf;jsessionid=BD56B50E26B2706C0AFAAEB53CF30279?text=&docid=218462&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=10385480): So soll nach der Auffassung des Europäischen Gerichtshofs keine wirksame Einwilligung vorliegen, wenn der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird. Daraufhin hat der Bundesgerichtshof am 28.05.2020 entschieden, dass ein Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf ((http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=107623&pos=0&anz=1).

In Kürze:

Bei Werbemaßnahmen muss der Verantwortliche sein berechtigtes Interesse an der Datenverarbeitung für Werbezwecke nachweisen können. Er muss eine Interessenabwägung durchführen und die „vernünftigen Erwartungen der betroffenen Person" in den Abwägungsprozess einbeziehen. Dabei kann auch zu berücksichtigen sein, ob bereits eine Geschäftsbeziehung zwischen den Beteiligten besteht („ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt").

Nach Auffassung der Aufsichtsbehörden (Datenschutzkonferenz, Kurzpapier Werbung - https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf) sprechen die Grundsätze einer fairen, dem Verarbeitungszweck angemessenen und einer für die betroffene Person nachvollziehbaren Verfahrensweise dagegen, Profile zur werblichen Ansprache (Werbescores) zu erstellen, die z. B. Informationen aus sozialen Netzwerken berücksichtigen. Eingriffsintensivere Maßnahmen wie Profilbildung würden außerdem dafür sprechen, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. Die Datenschutzkonferenz verweist zudem darauf, dass es sich noch zeigen muss, inwieweit es im Rahmen der Interessenabwägung in Europa gelingen wird, die in Deutschland entwickelten Maßstäbe auch unter Geltung der DSGVO aufrechtzuerhalten.

Die Datenschutzkonferenz hat im März 2019 außerdem eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

Weiterhin muss abgewartet werden, wann und ob die die ePrivacy-Verordnung verabschiedet wird. Die ePrivacy-Verordnung umfasst spezielle Regelungen zum Umgang mit Daten durch elektronische Kommunikationsdienste (z.B. Cookies).