DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

Dossier I - Das „neue“ Datenschutzrecht

November 2018

Prof. Dr. Anne Riechert

In diesem Dossier erfolgt ein Überblick über Änderungen im Datenschutzrecht. 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 (Dossier II und Dossier III)

B. Dokumentationspflichten und Verzeichnis von Verarbeitungstätigkeiten (Dossier IV)

C. Datenschutz-Folgenabschätzung (Dossier V)

D. Datenschutzbeauftragter (Dossier VI)

E. Auftragsverarbeitung (Dossier VII)

F. Übermittlung personenbezogener Daten an Drittländer (Dossier VIII)

G. Transparenz der Datenverarbeitung (Dossier IX und Dossier X)

H. Werbung (Dossier XI)

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 Verordnung (EU) 2016/679“ inzwischen 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).

Die Meldepflichten bei Datenschutzverletzungen begrenzte das BDSG-alt auf Fälle der unberechtigten Übermittlung von sensiblen Daten oder Kontodaten an Dritte. 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).

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. Die Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen verweist darauf, dass dies der Regelfall sein wird, da die Verarbeitung in den meisten Fällen nicht nur gelegentlich erfolge (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html – Stand: August 2018. Achtung - Update: Link ist nicht mehr erreichbar. Die Aufsichtsbehörde stellt nunmehr ausschließlich die Hinweise der Datenschutzkonferenz zum Abruf bereit, aus denen sich jedoch entsprechendes entnehmen lässt: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf).

Auch sobald ein Daten verarbeitender Betrieb Lohn-und Gehaltsdaten mit dem Merkmal „Religionszugehörigkeit" (bedingt durch die Kirchensteuergesetze zwingend) versieht, sei gemäß der Ausführungen der Landesbeauftragten Nordrhein-Westfalen die Rückausnahme „besondere Arten von Daten" gegeben, was zur Dokumentationspflicht führe (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html – Stand: August 2018. Achtung - Update: Link ist nicht mehr erreichbar. Die Aufsichtsbehörde stellt nunmehr ausschließlich die Hinweise der Datenschutzkonferenz

zum Abruf bereit: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf. Hierin heißt es: *„Bei Verarbeitungen, die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (z. B. Bonitätsscoringverfahren, Betrugspräventionsverfahren) oder besondere Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (Religionsdaten, Gesundheitsdaten, biometrische Daten zur eindeutigen Identifizierung etc.) oder über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO betreffen oder nicht nur gelegentlich erfolgen (alle sonstigen Verarbeitungen, z. B. Lohnabrechnungen, Kundendatenverwaltung, IT-/Internet-/E-Mail-Protokollierung, Schulnoten). Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten drei Fallgruppen erfüllt ist.“*).

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen empfiehlt zudem, weitere, dem Verständnis des Verarbeitungsverzeichnisses dienende, Informationen zur Dokumentation datenschutzrelevanter Vorgänge außerhalb des Verarbeitungsverzeichnisses zu erstellen und vorzuhalten (z. B. ein Sicherheits-und Rechte-und-Rollen-Konzept, ein Wiederanlaufkonzept sowie die Dokumentation des Ergebnisses einer gegebenenfalls durchgeführten Datenschutz-Folgenabschätzung), um den Anforderungen aus Artikel 24 gerecht zu werden (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html - Stand: August 2018. Achtung - Update: Link ist nicht mehr erreichbar – letzter Aufruf: August 2018. Die Aufsichtsbehörde stellt nunmehr ausschließlich die Hinweise der Datenschutzkonferenz zum Abruf bereit, aus denen sich jedoch entsprechendes entnehmen lässt. Es erfolgt allerdings der Hinweis, dass Redundanzen zu vermeiden sind: “*Um Redundanzen zu vermeiden und den Aufwand für die Erstellung und Führung des Verzeichnisses zu reduzieren, können in die einzelnen Beschreibungen Verweise auf bestehende Dokumente aufgenommen werden.*“ - https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf).

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, was jedoch ein elektronisches Format umfasst.

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 zukünftig 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 und er war bereits Prüfbestandteil der Vorabkontrolle nach BDSG-alt. Zu beachten ist nun jedoch, dass die Prüfung im europäischen Kontext vorgenommen werden muss. Daher sind die Regelungen der Europäischen Menschenrechtskonvention mit einzubeziehen und insgesamt alle Grundrechte, die durch das Datenschutzrecht mittelbar geschützt werden.

In diesem Zusammenhang hat die Datenschutzkonferenz 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 geplanten 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 V 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 sollen zu diesem Zweck eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Die Links zu diesen Listen sind im Dossier V Datenschutz-Folgenabschätzung enhalten.

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.

Eine Dokumentation im Sinne einer „Schwellenwertanalyse“ ist ebenso erforderlich, wenn der Verantwortlich zu dem Ergebnis gelangt, dass kein Risiko für die Rechte und Freiheiten der betroffenen Personen vorliegt.

D. Datenschutzbeauftragter

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 10 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind. Ein im Auftrag des Berufsverbands der Datenschutzbeauftragten Deutschland (BvD) veröffentlichtes Gutachten geht im Übrigen nicht davon aus, "*dass die Regelung des BDSG-neu in Widerspruch zum Regelungsgehalt der Datenschutzgrundverordnung steht*" (https://www.bvdnet.de/wp-content/uploads/2017/11/DMP-BvD-e.V.-gutachterliche-Stellungnahme-31.07.2017.pdf).

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_DS-GVO_1.pdf). Für Praxen, die ein einzelner Arzt betreibt, soll nach Auffassung von deutschen Aufsichtsbehörden diese Verpflichtung regelmäßig entfallen, so dass die 10-Personen-Grenze des BDSG-neu gilt (Entschließung der Datenschutzkonferenz vom 26.04.2018 - https://www.datenschutz-bayern.de/dsbk-ent/DSK_95-DSB-Bestellpflicht.pdf). Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) verweist darauf, dass auch der Arzt selbst zu den Personen zählen soll, die bei der Prüfung der „Zehn-Personen-Regel" zu berücksichtigen seien (https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html).

- **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_DS-GVO_1.pdf).

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 V 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 der Artikel-29-Datenschutzgruppe vertritt die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Auffassung (S.9), dass auch zukünftig ausschließlich eine natürliche Person (keine juristische Person) als Datenschutzbeauftragter zu benennen ist. Hierzu wird angemerkt, dass die unterschiedlichen Auffassungen zur Benennung eines Datenschutzbeauftragten ab Mai 2018 verbindlich geklärt werden können (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Datenschutzbeauftragte_nach_der_DS-GVO_und_der_JI-RL/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 Haftung des Datenschutzbeauftragten beinhalten (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Datenschutzbeauftragte_nach_der_DS-GVO_und_der_JI-RL/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-neu** ist ein Datenschutzbeauftragter zu benennen, wenn mindestens 10 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, so dass

die 10-Personen-Grenze des BDSG-neu gilt. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) verweist darauf, dass auch der Arzt selbst zu den Personen zählen soll, die bei der Prüfung der „Zehn-Personen-Regel“ zu berücksichtigen seien.

E. Auftragsverarbeitung

Das Instrument der Auftragsverarbeitung (Artikel 28 DSGVO) 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. 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).

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.

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.

Entsprechend dem bisherigen Recht kann das angemessene Datenschutzniveau 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 gilt einschränkend für die Unternehmen, die sich verpflichtet haben, den Datenschutzstandard des EU-US Privacy Shield einzuhalten, so dass diese Regelungen ebenso nach US-Recht durchsetzbar sind (siehe https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf sowie https://eur-lex.europa.eu/legal-

content/DE/TXT/HTML/?uri=CELEX:32016D1250&from=DE). Nähere Details sind dem Dossier VIII Übermittlung personenbezogener Daten an Drittländer zu entnehmen. Im Übrigen handelt es sich gemäß einer Mitteilung der Europäischen Kommission vom Januar 2018 bei dem Vereinigten Königreich ab 30.03.2019 ebenso um ein Drittland. Bislang ist allerdings noch kein Angemessenheitsbeschluss seitens der Europäischen Kommission erfolgt. Siehe die Mitteilung der Europäischen Kommission, abrufbar unter: http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

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.

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.

Die Artikel-29-Datenschutzgruppe vertritt hierzu die Auffassung, dass diese Ausnahmen eng auszulegen sind (WP 261vom 06.02.2018-
http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49771).

In Kürze:

Übermittelt der Verantwortliche personenbezogene Daten in Länder außerhalb der EU/EWR (Drittländer/Drittstaaten), muss wie nach bisherigem Recht 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“.

In Bezug auf die Übermittlung von Daten in die USA aufgrund des EU-US Privacy Shield geht der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz davon aus, dass dieses trotz der von den Datenschutzaufsichtsbehörden geäußerten Kritik als Grundlage genutzt werden kann, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, die sich gemäß dem Privacy Shield zertifiziert haben (https://www.datenschutz.rlp.de/de/themenfelder-themen/privacy-shield/).

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 im Gegensatz zum BDSG-alt nunmehr 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 der Artikel-29-Datenschutzgruppe zu verweisen, die keinen Unterschied zwischen den Informationspflichten des Absatz 1 und Absatz 2 macht (WP 260, S. 12 - http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025). 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.

Nähere Details können dem Dossier IX Informationspflichten und dem Dossier X Auskunftsrechte entnommen werden.

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.

Auch wenn bereits unter dem BDSG-alt die Auffassung galt, dass ein Auskunftsantrag der betroffenen Person zeitnah zu bearbeiten ist, ist nun in der DSGVO für die Erfüllung sämtlicher Betroffenenrechte, die mittels Antrag geltend gemacht werden, eine Frist von einem Monat vorgesehen, 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

Das so genannte Listendatenprivileg des BDSG-alt existiert nicht mehr. Werbemaßnahme müssen nunmehr mit „berechtigten Interessen“ (Artikel 6 Absatz 1f DSGVO) des Verantwortlichen begründet werden. Grundsätzlich kann gemäß Erwägungsgrund 47 der DSGVO die Direktwerbung ein solches berechtigtes Interesse des Verantwortlichen darstellen.

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.lda.bayern.de/media/dsk_kpnr_3_werbung.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.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/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.

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.lda.bayern.de/media/dsk_kpnr_3_werbung.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.

Insgesamt sind europaweit geltende Verhaltensregeln angestrebt und es werden Leitlinien des Europäischen Datenschutzausschusses erwartet.

Weiterhin müssen die Trilogverhandlungen zur ePrivacy-Verordnung abgewartet werden. Die ePrivacy-Verordnung umfasst spezielle Regelungen zum Umgang mit Daten durch elektronische Kommunikationsdienste (z.B. Cookies).