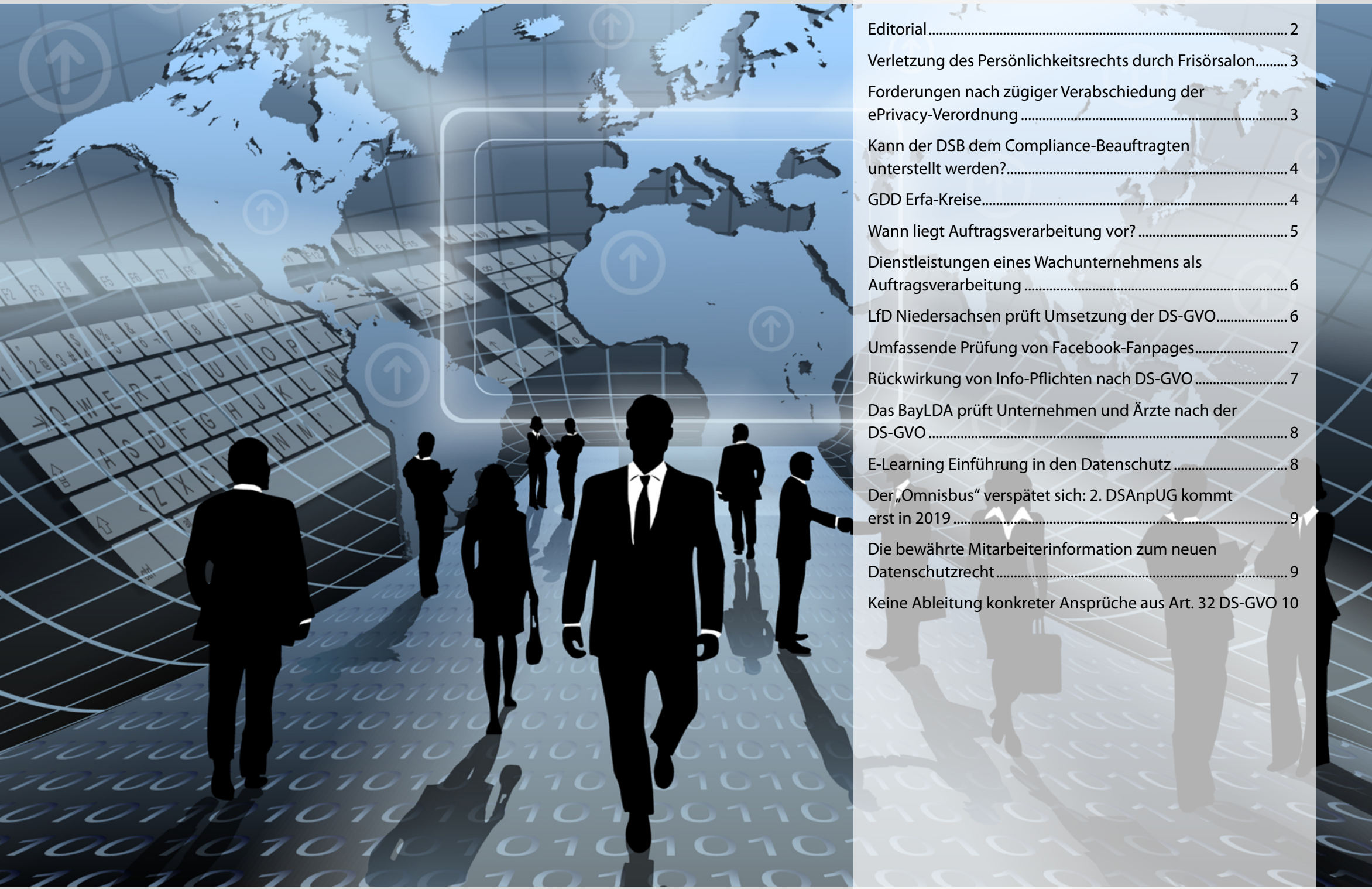
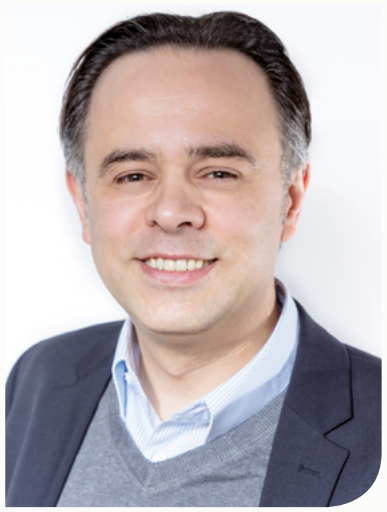
Datenschutz
newsbox

Ausgabe
11
2018



DATAKONTEXT



Editorial

Erklärtes Ziel der DS-GVO ist es, einen soliden, kohärenten und klar durchsetzbaren Rechtsrahmen in der Union zu schaffen. In Anbetracht der zahlreichen Öffnungsklauseln scheint das Ziel einer Vollharmonisierung schwierig erreichbar zu sein. Dabei ist dem europäisches Datenschutzausschuss eine entscheidende Rolle zugewiesen. Die Kernaufgabe des Ausschusses ist es, die einheitliche Anwendung der DS-GVO innerhalb der EU sicherzustellen. Zudem kann er im sogenannten Kohärenzverfahren rechtsverbindliche Beschlüsse zu der Frage fassen, ob ein Verstoß gegen die DS-GVO vorliegt.

Der deutsche Anwender des Datenschutzrechts wäre aber oftmals schon zufrieden, wenn zumindest unter den hiesigen Aufsichtsbehörden immer eine einheitliche Sichtweise gegeben wäre.

Das LDI NRW (http://t1p.de/ewvo) geht bspw. im Falle der reinen Lohn- und Gehaltsabrechnung oder bei sonstigen, rein technischen Dienstleistungen auch bei Steuerberatern von einer AV aus. Das BayLDA (http://t1p.de/82g6) hingegen sieht auch bei reiner Lohnbuchhaltung eine eigene Verantwortung der Steuerberater aufgrund des Steuerberaterrechts als gegeben an. Die Bundessteuerberaterkammer weist in Ihrem aktualisierten Leitfaden vom Oktober 2018 (Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften, Ziffer 7.3) auf den Umstand hin, dass die Einbeziehung eines Berufsgeheimnisträgers (StB, RA, WP, externe Betriebsärzte), Inkassobüros mit Forderungsübertragung, Bankinstituts für den Geldtransfer, Postdienstes für den Brieftransport etc. keine Auftragsverarbeitung darstellt. Es handele sich um die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen. Für die Verarbeitung (einschließlich Übermittlung) personenbezogener Daten müsse eine Rechtsgrundlage gem. Art. 6 DS-GVO gegeben sein, z. B. die Einwilligung der betroffenen Person oder die Wahrung berechtigter Interessen des Verantwortlichen (Kanzlei).

Die Abweichung in der Rechtsaufassung liegt hierbei nicht in Nuancen; diese stehen sich diametral gegenüber. Für den Rechtsanwender ist das ärgerlich, zumal diese „Disharmonie“ der Aufsichtsbehörden vermeidbar wäre, meint

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Verletzung des Persönlichkeitsrechts durch Frisörsalon

Das Landgericht Frankfurt am Main hat mit seinem Urt. v. 13.09.2018 bestätigt, dass ein Friseurgeschäft, dass Videos von Haarverlängerungen ihrer Kunden erstellt und über das Netz zum Abruf bereitstellt, sowohl gegen das KUG als auch gegen die Datenschutzgrundverordnung verstößt. Die Parteien streiten über Ansprüche wegen Verletzung des Persönlichkeitsrechts durch eine Bildnisveröffentlichung.
Der Verfügungsbeklagte (nachfolgend: Beklagter) betreibt einen Frisörsalon in Frankfurt am Main. Am 29.06.2018 begab sich die Verfügungsklägerin mit ihrem Lebenspartner in den Frisörsalon des Beklagten, um eine Haarverlängerung vornehmen zu lassen. Während der Behandlung fotografierte ein der Klägerin unbekannter Mann die Klägerin. Zudem wurde das streitgegenständliche Video, auf dem die Klägerin erkennbar ist, erstellt.
Kurze Zeit später stellte die Klägerin fest, dass der Beklagte am 04.07.2018 (16:42 Uhr) auf seiner Facebook Fanpage unter anderem das streitgegenständliche Video postete/veröffentlichte, auf dem die Klägerin klar und eindeutig erkennbar war. Auf der Facebook Seite befanden sich zum damaligen Zeitpunkt auch Lichtbilder der Klägerin. Die Klägerin forderte den Beklagten persönlich auf, die Lichtbilder und das Video zu entfernen. Der Beklagte kam der Aufforderung lediglich hinsichtlich der Lichtbilder nach, hinsichtlich des Videos reagierte er – trotz des anwaltlichen Schreibens – vorgerichtlich nicht. Die Kammer hat dem Beklagten durch einstweilige Verfügung untersagt, das Bildnis der Klägerin in Form eines Fotos oder als Filmaufnahme/Video öffentlich zur Schau zu stellen, wie dies auf der Website geschehen ist. Gegen den Beschluss hat der Beklagte mit Schriftsatz vom 22.08.2018 Widerspruch eingelegt.
Das OLG Frankfurt am Main bestätigt die einstweilige Verfügung der Kammer. Die Klägerin könne von dem Beklagten die Unterlassung der weiteren Veröffentlichung des streitgegenständlichen Videos aus den §§ 823, 1004 BGB, 22 f. KUG bzw. Art. 6 Abs. 1 DS-GVO, jeweils i.V.m. Art. 79 Abs. 1, 85 DS-GVO verlangen.
Insoweit könne letztlich offen bleiben, ob die §§ 22, 23 KUG als Normen im Sinne von Art. 85 Abs. 1 DS-GVO (VO (EU) 2016/679), die am 25.05.2018 Geltung erlangt hat und nationale Regelungen zum Datenschutz grundsätzlich verdrängt, für Fälle wie den vorliegenden, der nicht unter journalistische, wissenschaftliche, künstlerische oder literarische Zwecke im Sinne von Art. 85 Abs. 2 DS-GVO fällt, weiter gelte oder nicht. Denn sowohl nach den §§ 22, 23 KUG als auch unter Berücksichtigung von Art. 6 Abs. 1 lit. a), f), 7 DS-GVO war die Veröffentlichung rechtswidrig.
Zu Gunsten des Beklagten greife insbesondere nicht die Haushaltsausnahme gemäß Art. 2 Abs. 2 lit. c) DS-GVO, da die streitgegenständliche Veröffentlichung nicht im Rahmen ausschließlich persönlicher Verarbeitung erfolgte, sondern im gewerblichen Kontext und zudem öffentlich im Internet.

Quelle: Landgericht Frankfurt am Main — Urt. v. 13.09.2018

Forderungen nach zügiger Verabschiedung der ePrivacy-Verordnung

Das „Netzwerk Datenschutzexpertise" ist ein Zusammenschluss von DatenschutzexpertInnen, deren Ziel es ist, öffentliche Diskussionen über Fragen des Datenschutzes sowie generell des Schutzes von Menschenrechten und Grundrechten in der digitalen Welt zu initiieren bzw. durch eigene Beiträge wissenschaftlicher oder praxisbezogener Art voranzubringen. Dabei sollen informationstechnische, rechtliche, sozioökonomische sowie weitere relevante Aspekte behandelt werden.
In einem Offenen Brief fordern 16 Nichtregierungsorganisationen (NGOs), darunter das Netzwerk Datenschutzexpertise, die Bundesregierung auf, im EU-Rat dafür zu sorgen, dass die Verhandlungen über die geplante Datenschutzverordnung für elektronische Kommunikation (ePrivacy-Verordnung) zeitnah abgeschlossen werden. Damit sollen der digitale Wettbewerb und die Bürgerrechte im Internet geschützt werden. Die bisher weitgehend unkontrollierte Überwachung der Internetnutzenden soll wirksam unterbunden werden.
Die Forderungen an den Gesetzgeber adressieren folgende Punkte:

- Stärkung des Rechtsrahmens für elektronische Kommunikation
- Schutz der Privatsphäre und des Wettbewerbs
- Sicherung der Privatsphäre durch Technikgestaltung und Voreinstellung
- Schutz vor Tracking Walls
- Verhinderung von Massenüberwachung und Vorratsdatenspeicherung

Quelle: Netzwerk Datenschutzexpertise

Kann der DSB dem Compliance-Beauftragten unterstellt werden?

Frage des GDD Erfa-Kreises Würzburg
Ich bin Datenschutzbeauftragter in einem Unternehmen. Immer wieder stellen sich hierbei Fragen bezüglich der Unternehmensstruktur, ob der Datenschutzbeauftragte im Compliance-Bereich eingegliedert und hierarchisch dem Compliance-Beauftragten unterstellt werden könnte oder ob er direkt unter der Geschäftsleitung anzusiedeln wäre. Nach neuer Rechtslage gemäß Art 38 Abs. 3 DS-GVO müsste der Datenschutzbeauftragte an die „höchste Managementebene" des Verantwortlichen berichten. Als Anlage ist eine Zitatensammlung mit Stimmen aus der Literatur und von Aufsichtsbehörden beigefügt.

Es bestehen daher folgende Fragen:

- Kann der Datenschutzbeauftragte dem Compliance-Beauftragten unterstellt werden oder ist dieser direkt der Geschäftsleitung zu unterstellen?
- Führen die neuen gesetzlichen Regelungen ab Mai 2018 zu einem anderen Ergebnis als nach alter Rechtslage?

Antwort des BayLDA:
In unserem Tätigkeitsbericht 2009/2010 haben wir unter Nr. 3.1 zur bisherigen BDSG-Rechtslage u. a. folgendes geschrieben:
Nach dem Bundesdatenschutzgesetz ist der Beauftragte für den Datenschutz dem Leiter der nicht-öffentlichen Stelle – ohne Zwischenebenen – unmittelbar zu unterstellen.

- Der Leiter muss die Vorgesetztenfunktion in vollem Umfang wahrnehmen, so zum Beispiel die Personalaufsicht und die disziplinarische Zuständigkeit ebenso wie die Zuteilung des erforderlichen Budgets. Der Datenschutzbeauftragte darf nicht mehreren Personen unterstellt sein.
- Zwischen dem Datenschutzbeauftragten und der Unternehmensleitung dürfen sich keine Zwischenebenen befinden. Sinn der gesetzlich vorgeschriebenen unmittelbaren Unterstellung des Datenschutzbeauftragten unter den Leiter der nicht-öffentlichen Stelle ist, dass der Datenschutzbeauftragte seine Aufgaben unbeeinflusst, unabhängig und weisungsfrei wahrnehmen kann und einen „ungefilterten" Zugang zum Leiter hat. Damit wäre nicht vereinbar, wenn er in seiner Funktion in eine weitere Organisationseinheit eingegliedert ist. Denn bei dieser vorgesetzten Stelle können leicht Interessenkonflikte zwischen dem Datenschutz und den weiteren Aufgaben auftreten, die das Gesetz mit der unmittelbaren Unterstellung des Datenschutzbeauftragten unter den Leiter der nicht-öffentlichen Stelle vermeiden wollte.
- Die Zuordnung des Datenschutzbeauftragten zur Unternehmensleitung muss im Organigramm klar erkennbar sein. Das ist weiterhin unsere Idealvorstellung von der besten Einordnung eines DSB in ein Unternehmen, damit dieser möglichst effektiv und unabhängig tätig werden kann. Die DS-GVO legt in Art. 38 Abs. 3 Satz 3 fest, dass der DSB unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters berichtet. Was daraus genau für die Stellung des DSB abgeleitet werden kann, über die rein formale direkte Berichtslinie an die Unternehmensleitung hinaus, wird im Moment noch unterschiedlich diskutiert. Wir drängen jedenfalls bei unseren Kontakten mit Unternehmen darauf, die DSB-Funktion möglichst effektiv auszugestalten.

GDD Erfa-Kreise

Die GDD hat zur Durchführung ihrer Aufgaben regionale Erfahrungsaustauschkreise (Erfa-Kreise) gebildet. In den über das ganze Bundesgebiet verteilten, z.Z. 30 Erfa-Kreisen, werden aktuelle Datenschutz- und Datensicherheitsprobleme diskutiert.
>> weitere Infos

Wann liegt Auftragsverarbeitung vor?

Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag des Verantwortlichen und auf Basis seiner Weisungen. Da die Leistungen eines Dienstleisters sehr vielschichtig sind, muss im Rahmen einer Einzelfallprüfung untersucht werden, ob eine Verarbeitung personenbezogener Daten im Auftrag vorliegt (GDD-Praxishilfe XII - Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO).
Es bestehen jedoch Kriterien (vgl. Weiterführende Hinweise der Artikel-29-Datenschutzgruppe in Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ vom 16.02.2010 (WP169), die bei der Prüfung zur Einordnung als Verantwortlicher oder Auftragsverarbeiter Unterstützung leisten können. So kann eine Stelle, die über die Zwecke der Verarbeitung personenbezogener Daten entscheidet, kein Auftragsverarbeiter sein. Bei der Beurteilung dieses Kriteriums ist zu untersuchen:

- welchen Umfang der Handlungsspielraum des Dienstleisters bei der Auftragsverarbeitung hat,
- wie der Dienstleister durch den Auftraggeber überwacht wird,
- die Expertise des Dienstleistes bei der Auftragsverarbeitung,
- die Transparenz des Dienstleisters gegenüber dem Betroffenen.

Gleiches gilt für eine Stelle, die über die wesentlichen Mittel einer Verarbeitung entscheidet.
Eine Entscheidung über „wesentliche Mittel“ einer Datenverarbeitung liegt in der Regel bei einem der folgenden Punkte vor:

- welche Daten verarbeitet werden
- wie lange sie verarbeitet werden
- wer Zugang zu ihnen hat, die alleinige Entscheidung des Auftragsverarbeiters über technisch-organisatorische Mittel ist kein Ausschlussgrund für eine Auftragsverarbeitung.

Stellt sich die Bewertung, ob es sich bei der zu betrachtenden Dienstleistung um eine Auftragsverarbeitung oder um eine sonstige Outsourcing-Lösung handelt, als schwierig dar, so können verschiedene Indizien (vgl. 3 Franck, Studienheft Nr. 385 —Datenschutzrecht, 2. Aufl. 2018, Bad Sooden, S. 41.) für eine klarere Unterscheidung herangezogen werden:

- Eine bestehende Weisungsabhängigkeit zwischen dem Auftraggeber und dem Dienstleister spricht für das Vorliegen einer Auftragsverarbeitung.
- Stellt sich die relevante Datenverarbeitung nicht als die Hauptleistung des Dienstleisters, sondern vielmehr als eine reflexartige Nebenerscheinung für die Erbringung einer davon unabhängigen Leistung dar, kann dies als Indiz für eine Übermittlung berücksichtigt werden.
- Hat der Auftragnehmer ein eigenes wirtschaftliches Interesse an den Daten oder dem Ergebnis der Datenverarbeitung, kann dies als weiteres Indiz für eine Übermittlung betrachtet werden.
- Ein eigenes rechtliches Verhältnis zwischen Auftragnehmer und Betroffenen kann ebenfalls ein Anhaltspunkt dafür sein, dass keine Auftragsverarbeitung, sondern eine Übermittlung im Vordergrund steht.
- Kommt eine Haftung des Auftragsnehmers für die Richtigkeit oder Rechtmäßigkeit der Datenverarbeitung in Frage, spricht auch dies eher für das Vorliegen einer Übermittlung.

Wird der Dienstleister mit der IT-Wartung oder Fernwartung betraut und besteht hierbei die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten des Auftraggebers, soll es sich nach Meinung der hiesigen Aufsichtsbehörden um eine Form der Auftragsverarbeitung handeln und die Anforderungen des Art. 28 DS-GVO sollen für die geschuldete Tätigkeit gelten (DSK Kurzpapier Nr. 13, S. 3.). Bei einer rein technischen Wartung ohne Zugriff auf personenbezogene Daten des Auftraggebers gelten die Vorgaben des Art. 28 DS-GVO entsprechend nicht.

Beispiele für Auftragsverarbeitungen sind:

- Cloud-Computing
- Newsletterversand
- Datenerfassung, Datenkonvertierung
- Auslagerung der Lohn- und Gehaltsabrechnung
- Backup-Auslagerung und Archivierung

Keine Auftragsverarbeitung stellen in der Regel dar:

- Tätigkeiten und damit verbundene Verarbeitungen personenbezogener Daten von Berufsgeheimnisträgern (Rechtsanwälte, Steuerberater, Wirtschaftsprüfer)
- Die Übertragung des Forderungsmanagements an ein Inkassounternehmen
- Postdienstleistungen in Form des Brieftransports

Dienstleistungen eines Wachunternehmens als Auftragsverarbeitung

Frage des GDD Erfa-Kreises Würzburg:
Ein Unternehmen (Wachunternehmen) führt die Einlasskontrolle in einem Produktionsunternehmen (Kunde) als externe Dienstleistung durch. Die Mitarbeiter des Wachunternehmens arbeiten auf Systemen des Kunden. Dabei werden einerseits Daten Einlass begehrender Personen mit den im System des Unternehmens gespeicherten Informationen abgeglichen, andererseits auch die Daten neuer Kontakte in das System des Kunden aufgenommen. Die Mitarbeiter müssen die Daten also zur Kenntnis nehmen, um die geschuldete Tätigkeit der Einlasskontrolle durchzuführen. Die Mitarbeiter sind nicht als überlassene Arbeitnehmer tätig, eine Geheimhaltungsvereinbarung ist geschlossen, die Mitarbeiter sind auf den Datenschutz verpflichtet.

- Ist ein AV-Vertrag erforderlich oder liegt eine bloße Nebenleistung vor?
- Ändert sich an der Antwort etwas, wenn die Mitarbeiter des Wachunternehmens streng nach den Vorgaben des Kunden vorgehen oder aber den Datenabgleich unter Berücksichtigung eigener Erfahrungswerte variieren (z. B. Tiefe der Prüfung im Sinne des Abgleichs von im Einzelfall mehr oder weniger Merkmalen?).

Antwort des BayLDA:
Externe Sicherheits-Dienstleister, die an der Pforte Besucher- und Anliefererdaten erheben, sind nach unserer Auffassung grundsätzlich Auftragsverarbeiter (vgl. die von uns veröffentlichte Übersicht zur Abgrenzung zwischen Auftragsverarbeitung und anderen Sachverhalten unter https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf). Dies würden wir in beiden angesprochenen Varianten so sehen, da in beiden Fällen nur das Produktionsunternehmen derjenige ist, der über die Zwecke und Mittel der Datenverarbeitung entscheidet und daher Verantwortlicher ist, nicht hingegen der Dienstleister.

LfD Niedersachsen prüft Umsetzung der DS-GVO

Knapp ein halbes Jahr nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) seine Prüfaktivitäten wieder verstärkt aufgenommen und neue flächendeckende Datenschutzkontrollen in Bayern angestoßen. Im Fokus der aktuellen Prüfungen steht der sichere Betrieb von Online-Shops, der Schutz vor Verschlüsselungstrojanern in Arztpraxen, die Erfüllung der Rechenschaftspflicht bei Großkonzernen und mittelständischen Unternehmen sowie die Umsetzung der Informationspflichten in Bewerbungsverfahren.
Eine Auswahl der vom BayLDA durchgeführten Kontrollen ist hier aufgelistet: https://www.lda.bayern.de/de/kontrollen.html
Auch die Landesbeauftragte für den Datenschutz Niedersachsen hat eine Prüfung bei insgesamt 150 Kommunen angestoßen. 150 niedersächsische Kommunen erhalten in diesen Tagen Post von der Landesbeauftragten für den Datenschutz (LfD). Ein knappes halbes Jahr nach Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) prüft Barbara Thiel, wie gut die Städte und Gemeinden ihre Arbeit an die neuen Anforderungen angepasst haben und wo sie noch nachbessern müssen. Dafür sollen die Kommunen Fragen zu vier Bereichen des Datenschutzes beantworten: Organisation, datenschutzkonforme Verarbeitung, Umgang mit Betroffenenrechten sowie mit Datenschutzverletzungen.
Den Fragebogen erhalten 12 Landkreise, 3 kreisfreie Städte, 3 große selbständige Städte, 87 Gemeinden sowie 45 Samtgemeinden in Niedersachsen. Anfang 2019 werden die Mitarbeiterinnen und Mitarbeiter der LfD die Antworten auswerten. Der Abschlussbericht soll dann im Frühjahr 2019 vorliegen.
Die Befragung der Kommunen ist die zweite große Prüfung der LfD seit Geltung der DS-GVO. Bereits Ende Juni hatte Thiel 50 große und mittelgroße niedersächsische Unternehmen aus verschiedenen Branchen angeschrieben. Der Bericht zu dieser Prüfung wird für Mai 2019 erwartet.

Umfassende Prüfung von Facebook-Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-201/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben. Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DS-GVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden.
Die DSK stellte fest, dass eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche) bislang nicht zur Verfügung gestellt worden sei. Auch Fanpage-Betreiberinnen und Betreiber müssten sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DS-GVO sei der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten werde, rechtswidrig.
Daher forderte die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehöre insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellten. Eine gemeinsame Verantwortlichkeit bedeute allerdings auch, dass Fanpage-Betreiberinnen und -Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem könnten Betroffene ihre Rechte aus der DS-GVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DS-GVO).
Kurz nach dem die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ihren Beschluss zu den sog. Facebook Fanpages veröffentlicht hat, kam Facebook den dort postulierten Anforderungen teilweise nach.
Nach der Veröffentlichung dieses Beschlusses hat Facebook ein Dokument mit dem den Titel „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ online gestellt. Obwohl Facebook nicht explizit darauf eingeht, ob diese Veröffentlichung als eine direkte Reaktion auf den Beschluss der DSK zu betrachten ist, ist nicht zu verkennen, dass Facebook mit diesem Dokument den Forderungen hinsichtlich einer Vereinbarung zur gemeinsamen Verantwortlichkeit nach der Art. 26 DS-GVO entgegen kommt.
Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat nun bekannt gegeben, dass sie seit Anfang November Anhörungsverfahren bei Stellen der Berliner Landesverwaltung, bei den politischen Parteien sowie bei einer Reihe von Unternehmen und Organisationen u. a. aus der Handels-, Verlags- und Finanzbranche in Sachen Facebook-Fanpages durchführt.
Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat allerdings Zweifel, dass die Informationen, die Facebook bisher – auch im Zusammenhang mit der veröffentlichten Ergänzungsvereinbarung – zur Verfügung gestellt hat, ausreichen, um Rechenschaft über die Rechtmäßigkeit der Verarbeitung der Daten von Besucherinnen und Besuchern der Fanpage ablegen zu können. Den Fragenkatalog im Anhörungsverfahren wird die Berliner Beauftragte für Datenschutz und Informationsfreiheit auf ihrer Webseite veröffentlichen.

Rückwirkung von Info-Pflichten nach DS-GVO

Frage des GDD Erfa-Kreises Würzburg:
Gem. Art. 13 DS-GVO müssen betroffene Personen bei Datenerhebung informiert werden. Viele Anwälte und auch die GDD vertreten die Auffassung, dass ab dem 25.05.2018 diese Pflicht gilt und diese keine Rückwirkung hat, denn die bereits erfolgten Datenerhebungen liegen lange in der Vergangenheit und etwaige Fristen wären sowieso verstrichen. Ist dies auch die Auffassung der Aufsicht?

Antwort des BayLDA:
Das WP 260 ist hier nicht ganz eindeutig. Tendenziell gehen allerdings wir davon aus, dass die Pflicht nicht rückwirkend besteht. Unabhängig davon, ob diese rechtlich notwendig ist, kann es sinnvoll sein, alle Bestandskunden gleichzeitig unabhängig von einer Erhebung zu informieren. Dann muss bei der tatsächlichen (Neu-)Erhebung nach DS-GVO nicht überprüft werden, ob bereits eine Information vorliegt oder nicht.

Das BayLDA prüft Unternehmen und Ärzte nach der DS-GVO

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) gibt an, dass es aktuell seine Prüfaktivitäten verstärkt. Die flächendeckenden Datenschutzkontrollen in Bayern fokussieren sich nach Angaben des BayLDA auf Prüfungen bei Online-Shops, bei Arztpraxen und in Bezug auf die Erfüllung der Accountibility-Pflichten würden Großkonzerne geprüft. Bei mittelständischen Unternehmen konzentrieren sich die Prüfungen auf die Umsetzung der Informationspflichten im Rahmen von Bewerbungsverfahren.

Im Rahmen der Prüfung der ausgesuchten Arztpraxen stand die Prüfung der Datensicherung im Vordergrund. Durch die Schadsoftware wie bspw. Verschlüsselungstrojaner werde der Zugriff auf Daten gesperrt und anschließend Lösegeld gefordert, um die Daten wieder im ursprünglichen Zustand zu erhalten. Meldungen über einen Befall von Arbeitsplatzrechnern bei bayerischen Verantwortlichen erreichen das BayLDA wöchentlich, so das BayLDA. Im Falle einer Infektion könne sich die Schadsoftware unter Umständen im gesamten Netzwerk der betroffenen Organisation ausbreiten. Ohne Datensicherung (Backups) könne nur in wenigen Fällen eine Wiederherstellung der Daten mühelos erfolgen.

Das BayLDA habe des Weiteren drei Großkonzernen jeweils 50 Fragen gestellt und prüft damit, ob in der jeweiligen Organisation eine datenschutzkonforme Verarbeitung personenbezogener Daten stattfindet und mit Betroffenenrechten sowie Datenschutzverletzungen richtig umgegangen wird. Ziel dieser Prüfung sei es also zudem festzustellen, inwieweit große Unternehmen in der Lage sind, die Einhaltung der gesetzlichen Vorgaben aus der DS-GVO auch nachzuweisen.

Bereits im Jahr 2015 habe das BayLDA in einer Großprüfung Unternehmen daraufhin kontrolliert, ob mit Bewerberdaten sachgemäß umgegangen wird. Dabei wurden einige Mängel vorgefunden, die erst im Rahmen der Aufarbeitung behoben wurden. Mit dieser Erfahrung entschied sich das BayLDA deshalb nun im Oktober 2018, erneut bei zufällig ausgewählten Verantwortlichen die Verarbeitung personenbezogener Daten in Bewerbungsverfahren zu untersuchen. Schwerpunkt sei dieses Mal, inwieweit die Informationspflicht gegenüber den Bewerbern korrekt umgesetzt wird und Bewerber letztendlich auch erfahren, wie mit ihren Daten umgegangen wird. Hierzu werden derzeit 15 Verantwortliche in Bayern, ausschließlich größere Betriebe und Vereine, geprüft.

In einer Prüfung zur allgemeinen Datenschutzorganisation waren darüber hinaus bei 15 KMUs 20 Fragen zu beantworten und zum Teil Unterlagen vorzulegen. Ein Schwerpunkt der Kontrolle stellte die Berücksichtigung des risikoorientierten Ansatzes der DS-GVO dar, der im Prinzip bedeutet, dass technische und organisatorische Schutzmaßnahmen entsprechend des Risikos aber auch nach der Größe und Art des Unternehmens auszuwählen sind.

Quelle: Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA)

Der „Omnisbus“ verspätet sich: 2. DSAnpUG kommt erst in 2019

Seit dem 25. Mai 2018 regelt die Datenschutz-Grundverordnung (DS-GVO) den Datenschutz in der gesamten Europäischen Union (EU) unmittelbar. Zur Vereinheitlichung des Datenschutzrechts genießt der Rechtsakt Anwendungsvorrang vor nationalen Regelungen. Trotzdem ist das nationale Recht dadurch nicht gänzlich obsolet geworden. Die sog. Öffnungsklauseln erlauben, aber zwingen die Mitgliedstaaten teilweise auch zum Erlass von einzelstaatlichem Recht.

Das 1. DSAnpUG kam pünktlich

Mit dem im Juni 2017 verabschiedeten 1. DSAnpUG hat der Bundesgesetzgeber die wohl wichtigste Anpassung und Umsetzung an die DS-GVO vorgenommen, indem er das Bundesdatenschutzgesetz (BDSG) grundlegend überarbeitet hat. Das BDSG konnte damit zeitgleich zur DS-GVO am 25.5. diesen Jahres Anwendung finden.

Das 2. DSAnpUG kommt zu spät

Mit erheblicherer Verspätung hat die Bundesregierung erst im September einen Gesetzentwurf für das 2. DSAnpUG vorgelegt. Damit soll das gesamte bundesdeutsche Recht DS-GVO-konform gestaltet werden. In dem vom Bundesinnenministerium (BMI) federführend zu verantwortenden sog. „Omnibus-Gesetz“ sollen in mehr als 150 Bundesgesetzen Änderungen vorgenommen werden. All diese Gesetze beinhalten bereichsspezifisches Datenschutzrecht, was der Änderung und Anpassung bedarf. Dabei handelt es sich beispielsweise um Gesetze wie das Antiterrordatei-Gesetz, das Bundesmeldegesetz, aber auch das Weingesetz oder das Schornstein-Handwerksgesetz sind betroffen.

Wie ist der weitere Gesetzgebungsverlauf?

In der nichtöffentlichen Sitzung des Innenausschusses des Deutschen Bundestages wurde am 7. November über die Durchführung einer öffentlichen Anhörung zu dem Gesetz beraten und entschieden. Das hat zur Folge, dass nun in der letzten Sitzungswoche des Bundestages, am 10. Dezember, eine parlamentarische Anhörung zu dem Thema durchgeführt wird. Da das DSAnpUG von Seiten des Bundesrats mitbestimmungspflichtig ist, bestimmt sich der Zeitplan der Gesetzgebung maßgeblich nach dem Sitzungskalender des Bundesrats. Dieser tagt in diesem Jahr am 14.12. das letzte Mal. Um das Gesetz dort auf die Tagesordnung zu bekommen, müsste der Bundestag nach der Anhörung am 10.12. das Gesetz spätestens am 13.12. in 2. und 3. Lesung im Parlament verabschieden. Dies wird in der Kürze der Zeit nicht zu leisten sein. Die erste Plenarsitzung des Bundesrats findet dann aber erst wieder am 15. Februar 2019 statt. Dieser Termin wird wohl zu schaffen sein und gibt auch dem Bundestag noch 3 weitere Sitzungswochen Zeit zur Entscheidung. Dadurch kann zunächst im zuständigen Ausschuss für Inneres und Heimat mit der gebotenen Sorgfalt und ausreichend Zeit eine Einigung herbeigeführt werden und im Anschluss kann die Abstimmung in 2./3. Lesung im Plenum gelingen.

Keine Ableitung konkreter Ansprüche aus Art. 32 DS-GVO

Nach Auffassung der österreichischen Datenschutzbehörde DSB lassen sich aus Art. 32 DS-GVO für den Betroffenen keine Ansprüche auf konkrete Sicherheitsmaßnahmen gegen den Verantwortlichen ableiten. Im konkreten Fall monierte die Betroffene, dass das Bundeskanzleramt und das österreichische Bundesministerium für Europa, Integration und Äußeres Daten und Informationen zum Sexualleben und Gesundheit („sensible persönliche Daten") in elektronischer Form über sie speichern würden.
Dem vordringlich geforderten Löschbegehren der Betroffenen wäre nach eigenem Bekunden der Betroffenen auch gedient, wenn eine Pseudonymisierung dieser Daten durchgeführt werden würde. Die unterlassene Pseudonymisierung sei eine Verletzung des Grundrechts auf Datenschutz. Es wäre unverhältnismäßig, wenn Daten in einer nicht pseudonymisierten Form aufbewahrt würden. Die Beschwerdeführerin befürchte, dass ihre Identität in den folgenden Jahrzehnten bei jedem Zugriff auf die Daten offengelegt werde, was nicht mehr mit dem öffentlichen Interesse begründet werden könne.
Insbesondere wären ihre Daten bei einem erfolgreichen Hacker-Angriff auf die Server der Beschwerdegegner sofort öffentlich zugänglich. Wenn Daten aufbewahrt werden würden, um „österreichische Rechtsansprüche" gegen die Neueinbringung einer gleichartigen Beschwerde durch sie bei einem anderen Tribunal zu verteidigen, dann werde der Dokumentationszweck durch die geforderte Pseudonymisierung nicht beschränkt. Auch aus der DS-GVO wäre abzuleiten, dass weitgehende Datenschutzmaßnahmen der Regelfall für die Archivierung sein müssten. So normiere Art. 5 Abs. 1 lit c DS-GVO das Prinzip der Datenminimierung und als Instrument dazu führe Art. 25 Abs. 1 DS-GVO die Pseudonymisierung an. Die Unterlassung dieser oder vergleichbarer Schutzmaßnahmen wäre ein mit dem Grundrecht auf Datenschutz unvereinbarer leichtfertiger Umgang mit sensiblen Daten.
Nach Auffassung der österreichischen Datenschutzbehörde könne in Bezug auf die von der Betroffenen gerügte Verletzung des Grundrechts auf Geheimhaltung durch eine „unterlassene Pseudonymisierung" aus der DS-GVO kein Recht abgeleitet werden, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen i.S.v Art. 32 DS-GVO von einem Verantwortlichen verlangen könnte. Ebenso wenig könne eine betroffene Person – wie von der Beschwerdeführerin begehrt – spezifische Maßnahmen zur Datenminimierung i.S.v Art. 5 Abs. 1 lit. c DS-GVO verlangen.
Wie nämlich aus Art. 32 DS-GVO ersichtlich sei, treffe die Verpflichtung zur Sicherheit der Verarbeitung personenbezogener Daten den Verantwortlichen bzw. den Auftragsverarbeiter, wobei diese Sicherheit – unter Berücksichtigung der in Abs. 1 dieser Bestimmung genannten Elemente – auf mehrere Arten gewährleistet sein könne.
Auch aus dem Blickwinkel einer systematischen Interpretation der DS-GVO könne nicht geschlossen werden, dass der Gesetzgeber einer betroffenen Person ein subjektives Recht auf Einhaltung bestimmter Datensicherheitsmaßnahmen gewähren wollte…». Im Ergebnis liege weder eine (bereits erfolgte) Verletzung des Grundrechts auf Geheimhaltung vor, noch könne eine spezifische Datensicherheitsmaßnahme (konkret: Pseudonymisierung) im Rahmen eines Beschwerdeverfahrens geltend gemacht werden.

Quelle: Bundesministerium für Digitalisierung und Wirtschaftsstandort