

Editorial	2
Unabhängiges Datenschutzzentrum Saarland veröffentlicht Tätigkeitsbericht	3
Bußgelder nach DS-GVO in der EU	3
VS-NfD Dokumente dürfen mit Gpg4win verschlüsselt werden	4
Hinweis auf Informationspflichten in E-Mail	4
Handbuch Beschäftigtendatenschutz (Anzeige)	4
Arbeitspapier zur großräumigen Standortverfolgung veröffentlicht	5
Pflicht zur Verschlüsselung bei Anwalt-eMails	5
Datenschutzrechtliche Vorgaben bei der Nutzung von Kameradrohnen	5
DSK: Nationale Benennungspflicht für DSB erhalten	6
Einführung in den Datenschutz (Anzeige)	6
Europäischer Datenschutzausschuss konkretisiert die Vertragserfüllung als Erlaubnistatbestand	7
DS-GVO verunsichert Bildjournalisten	7
EuGH prüft Klagebefugnis von Verbraucherverbänden	8
GDD-Forum – Ihr Dialog mit der Datenschutzaufsicht (Anzeige)	8
Personalüberlassung als Auftragsverarbeitung?	9
Forschungsbericht: Sanktionen der DS-GVO	9
Aufsichtsbehörde gibt Antworten zur Zulässigkeit von Cookies und Tracking	10
Kontaktdaten von B2B-Ansprechpartnern: Welche Rechtsgrundlage?	10



Editorial

Zum Thema "Selbstdatenschutz" kann der interessierte Leser bei Wikipedia erfahren, dass darunter, die durch den Einzelnen zum Schutz seines Rechts auf informationelle Selbstbestimmung ergriffenen technischen, organisatorischen und rechtlichen **Maßnahmen** verstanden werden. Dazu werden bisher in erster Linie Verhaltensweisen des Einzelnen gezählt, möglichst wenig Ansatzpunkte für eine Erhebung seiner Daten zu bieten. Dazu zählt auch, selbst aktiv Gegenmaßnahmen zu ergreifen.

Den (noch) zulässigen Rahmen des "Selbstdatenschutzes" und die Intensität möglicher Gegenmaßnahmen im Hinblick auf invasiv empfundene Grenzübertritte in die informationelle Selbstbestimmung hat das Amtsgericht Riesa jüngst neu ausgelotet, in dem es einen Mann freisprach, der mit einem Luftgewehr eine Drohne über seinem Garten **abgeschossen** hatte. Das Gericht sah den Abschuss durch den sog. Selbsthilfe-Paragrafen § 229 BGB gedeckt.

Auch demjenigen, der kein "Datenschutz-Schalk" ist, drängt sich die doch naheliegende Frage auf, wann es wohl bald die ersten Fälle von Selbsthilfe gegen Auto-Dashcams oder allzu neugierig horchende "Siris und Alexas" geben wird.

Wobei man erwähnen muss, dass zumindest ein allzu **fieser "Assistent"** von Amazon ein wenig Ärger verdient hätte, findet Ihr

Levent Ferik

Unabhängiges Datenschutzzentrum Saarland veröffentlicht Tätigkeitsbericht

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (UDZ Saarland), Monika Grethel, hat am 10. April 2019 dem Präsidenten des saarländischen Landtags Stephan Toscani und dem Ministerpräsidenten Tobias Hans den 27. Tätigkeitsbericht des Unabhängigen Datenschutzzentrums Saarland für die Jahre 2017/2018 überreicht und in einem anschließenden Pressegespräch der Öffentlichkeit vorgestellt. Die Landesbeauftragte des UDZ legt den Lesern den vorliegenden Tätigkeitsbericht und die dort geschilderten Fallgestaltungen als eine Hilfestellung bei der Ausgestaltung und Anpassung von Verfahren der Verarbeitung personenbezogener Daten ans Herz.

Beispielhaft sind folgende Themengebiete hervorgehoben:

- **Beschäftigtendatenschutz**
Ein Rückgriff auf private Chatprotokolle ist für disziplinarrechtliche Ermittlungen im Zusammenhang mit der Nebenbeschäftigung eines Polizeibeamten unzulässig (Kapitel 8.2). Die GPS Ortung von Fahrzeugen zur Mitarbeiterdisposition kann regelmäßig nicht auf die Einwilligung der betroffenen Beschäftigten gestützt werden (Kapitel 8.4)
- **Veröffentlichung von Bildaufnahmen**
Die Frage, ob und unter welchen Bedingungen Bildaufnahmen von Personen für Zwecke der Öffentlichkeitsarbeit verarbeitet werden dürfen, beschäftigte im Berichtszeitraum verschiedene Akteure. Für Kommunen gilt, dass diese ein legitimes Interesse an Öffentlichkeitsarbeit haben können. Soweit hierbei Bildaufnahmen von Veranstaltungsteilnehmern angefertigt und veröffentlicht werden, ist der datenschutzrechtliche Regelungsrahmen zu berücksichtigen (Kapitel 6.3, 6.3.1, 6.3.2, 6.3.3). Arbeitgeber können eine Veröffentlichung von Mitarbeiterfotos lediglich auf die Einwilligung der Betroffenen stützen. Dem Widerruf der Einwilligung des Beschäftigten

ist Rechnung zu tragen (Kapitel 8.7). Im Rahmen der Öffentlichkeitsarbeit von Vereinen kann eine Veröffentlichung von Veranstaltungs- oder Mitgliederfotos regelmäßig auch ohne Einwilligung der Betroffenen erfolgen (Kapitel 13.5.2).

- **Datenschutzbeauftragte**

Auch nach der neuen Rechtslage haben Unternehmen, Behörden und sonstige datenverarbeitende Stellen unter bestimmten Voraussetzungen verpflichtend Datenschutzbeauftragte zu benennen und dies der Datenschutzaufsichtsbehörde zu melden.

Dieser Meldepflicht kann im Saarland über ein elektronisches Meldeformular nachgekommen werden (Kapitel 9.1). Bei der Auslegung der gesetzlichen Vorgaben zur Bestellpflicht und deren organisatorischer Umsetzung können sich für Verantwortliche Unklarheiten ergeben. Schwierigkeiten bereiten im Berichtszeitraum vor allem die Fragestellungen, wann eine Verarbeitung personenbezogener Daten umfangreich ist, welche Personen im Unternehmen ständig automatisiert personenbezogene Daten verarbeiten und ob eine juristische Person als Datenschutzbeauftragter benannt werden kann (Kapitel 9.1.1, 9.1.2 und 9.1.3). Trotz der Verarbeitung von Gesundheitsdaten in erheblichem Umfang gilt für Einzelärzte oder bei Gemeinschaftspraxen eine Pflicht zur Benennung eines Datenschutzbeauftragten nur unter der Voraussetzung, dass in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind (Kapitel 9.2).

Quelle: *UDZ Saarland*

Bußgelder nach DS-GVO in der EU

Vor Kurzem ist ein neues DataAgenda-Arbeitspapier erschienen. Dieses widmet sich den seit der Datenschutz-Grundverordnung (DS-GVO) öffentlich gewordenen Bußgelder.

Das auf der [Seite der DataAgenda-Arbeitspapiere](#) zu findende [Arbeitspapier](#) beinhaltet eine Liste sämtlicher, uns bis zum 01.05.2019 bekannt

gewordener Bußgelder, die auf Grundlage der DS-GVO verhängen wurden. Die Auflistung zeigt, dass die Aufsichtsbehörden innerhalb der gesamten Europäischen Union (EU) im ersten Jahr der Anwendung der DS-GVO durchaus Gebrauch von dem finanziellen Sanktionsmechanismus machen.

VS-NfD Dokumente dürfen mit Gpg4win verschlüsselt werden

Das Bundesamt für Sicherheit in der Informationstechnik teilt mit, dass Behörden ab sofort auch mit der Geheimhaltungsstufe **VS-NfD** eingestufte vertrauliche Inhalte unter Verwendung des OpenPGP Standards verschlüsseln und austauschen dürfen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dazu erstmalig die Software Gpg4win für Microsoft Windows und eine Konfiguration von GnuPG für das unter Linux nutzbare E-Mail-Programm KMail zur Übertragung von Verschlusssachen der Einstufung "VS-Nur für den Dienstgebrauch (VS-NfD)" zugelassen.

"Durch die Zulassung des OpenPGP-Standards geben wir Behörden ein Werkzeug an die Hand, mit dem sie auch eingestufte Inhalte vertraulich austauschen können und unterstützen damit als nationale Cyber-Sicherheitsbehörde das Vorhaben der Bundesregierung, Deutschland zum 'Verschlüsselungsstandort Nr. 1' zu machen. Diesem Ziel sind wir wieder ein Stück näher gekommen", so BSI-Präsident Arne Schönbohm.

Unter Windows lassen sich mit Gpg4win einerseits über den Windows Explorer Dateien, sowie andererseits über das enthaltende Outlook Add-in E-Mails für die vertrauliche Kommunikation verschlüsseln und signieren. Zur Auswahl stehen dabei die Standardverfahren OpenPGP und S/MIME. Die Implementation ist vollständig im Quelltext als Open Source Software verfügbar.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Hinweis auf Informationspflichten in E-Mail

Frage des GDD-Erfa-Kreises Coburg:

Wenn ein Angebot an eine betroffene Person per E-Mail verschickt wird, ist es dann möglich bezüglich der Informationspflichten auf die Datenschutzerklärung zu verweisen oder müssen diese als z.B. PDF direkt der E-Mail angehängt werden?

Antwort des BayLDA:

Das WP 260 erlaubt eine "gestufte" Vorgehensweise. In der ersten Stufe sollte auf die Identität des Verantwortlichen, die Zwecke der Verarbeitung und das Bestehen von Betroffenenrechten hingewiesen werden; auch überraschende Verarbeitungen sollten genannt werden. In einer zweiten Stufe müssen dann alle Informationen unabhängig in welchem Absatz sie in Art. 13 und 14 gefordert werden, gegeben werden. Hierbei kann auf eine Datenschutzerklärung auf der Webseite verwiesen werden. Es muss dabei jedoch sichergestellt werden, dass nicht auf eine allgemeine "Datenschutzinformation für alle Fälle" verwiesen wird, sondern, dass der interessierte Betroffene insbesondere erkennt, was die Rechtsgrundlage der Verarbeitung in seinem speziellen Fall ist. Es kann daher im Zweifel keine "One-Size-Fits-All-Information" für alle betroffenen Personen also Beschäftigte, Kunden, Geschäftspartner, Webseitenbesucher und Lieferanten geben.

Anzeige

Buchtipps

Jetzt neu: Handbuch Beschäftigtendatenschutz

Prof. Golas neu konzipiertes Datenschutzhandbuch – unverzichtbar für alle, die mit Personaldaten arbeiten.



- **Praxisnah:** ausführliche Fallbeispiele und konkrete Lösungsansätze
- **Etabliert:** 8. aktualisierte und erweiterte Auflage
- **Informativ:** ausgewertete Stellungnahmen der Aufsichtsbehörden

»Jetzt bestellen

»Blick ins Buch


DATAKONTEXT

Arbeitspapier zur großräumigen Standortverfolgung veröffentlicht

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group), die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Maja Smolczyk, geleitet wird, hat auf ihrer 64. Sitzung am 29. und 30. November 2018 in Queens-town (Neuseeland) ein Arbeitspapier zur großräumigen Standortverfolgung verabschiedet.

Technologien zur Standortverfolgung bieten Vorteile und Chancen, die von öffentlichem Interesse sind. So können Daten von Geräten, die in Autos eingebaut sind, beispielsweise verwendet werden, um die Straßennutzung effizienter zu gestalten, die CO₂-Emissionen zu reduzieren oder die Sicherheit von Fahrern und Fußgängern zu verbessern. Die permanente Nutzung des Mobilfunks und anderer drahtloser Netze, die eine physische Standortverfolgung ermöglichen, z. B. beim Wandern, Joggen, Auto- oder Radfahren führt jedoch dazu, dass die Nachverfolgbarkeit alltäglicher Aktivitäten der Menschen

immer mehr zur Norm wird. Das birgt große Risiken für das Recht der betroffenen Personen auf Achtung ihres Privatlebens und mittelbar die Wahrnehmung weiterer Menschen- und Freiheitsrechte.

Das Arbeitspapier zur großräumigen Standortverfolgung untersucht die Risiken für den Datenschutz und die Privatsphäre, die mit der groß angelegten Erhebung von Standortdaten im öffentlichen oder privaten Interesse verbunden sind. Es enthält Empfehlungen an Unternehmen, Industrie und Behörden zum rechtmäßigen Einsatz solcher Technologien sowie zu möglichen technischen und organisatorischen Vorkehrungen, um die von ihnen ausgehenden Risiken zu minimieren. Das Arbeitspapier ist in englischer Sprache unter <http://www.berlin-privacy-group.org> abrufbar. Eine deutsche Übersetzung wird in Kürze auf der Webseite der Berliner Beauftragten für Datenschutz und Informationsfreiheit veröffentlicht.

Pflicht zur Verschlüsselung bei Anwalt-eMails

Die Frage, ob Anwältinnen und Anwälte unverschlüsselt per E-Mail mit Mandanten kommunizieren dürfen, ohne gegen die Pflicht zur Verschwiegenheit zu verstoßen, war in jüngster Vergangenheit öfter ein Streitpunkt. Datenschutz-Aufsichtsbehörden betrachteten die Fragestellung noch genereller und stellten diese Frage für jegliche Berufsgeheimnisträger, so bspw. auch für Ärzte (Tätigkeitsbericht 2017/18 – Bayerisches Landesamt für Datenschutzaufsicht, S. 94, Ziffer 16.7).

Zumindest für die Rechtsanwälte könnte es ein wenig mehr Rechtssicherheit in dieser Sache geben. Ein Beschluss der letzten Satzungsversammlung der Bundesrechtsanwaltskammer (BRAK) hat dafür den Weg geebnet. In § 2 der Berufsordnung der Rechtsanwälte soll es eine neue Regelung zur Verschwiegenheit geben, der Regelungen enthält, wann Anwältinnen und Anwälte bei Risiken für die Vertraulichkeit von der Zustimmung ihrer Mandanten ausgehen dürfen und wann es erforderlich ist, dem Mandanten einen Warnhinweis diesbezüglich zu geben.

Quelle: Deutscher Anwaltverein e.V. (DAV)

Datenschutzrechtliche Vorgaben bei der Nutzung von Kameradrohnen

Neben den Normen der Luftverkehrs-Verordnung (LuftVO) können Nutzer sog. Kameradrohnen auch mit datenschutzrechtlichen Vorschriften konfrontiert sein. Sind die Drohnen mit Kameras ausgestattet, ermöglichen sie unbeobachtete Blicke in nicht einfach zugängliche Orte wie den Garten oder auf die Sonnenterrasse des Nachbarn, aber auch auf öffentliche Straßen oder Plätze. Dabei handelt es sich um eine Datenverarbeitung mittels Videoüberwachung. Datenschutzrechtliche Vorgaben der DS-GVO werden relevant, sobald eine Datenverarbeitung nicht ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgt, sondern z. B. zu gewerblichen Zwecken oder zum Zwecke der Veröffentlichung. Neben dem aufsichtsbehördlichen Verfahren steht Betroffenen auch der Zivilrechtsweg offen. Bei einem Grundrechtseingriff kann u. U. ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) geltend gemacht werden. Strafrechtliche Belange können eine Rolle spielen, wenn der Drohneinsatz zur Verwirklichung von Straftatbeständen führt.

Weitere Details lassen sich dem Positionspapier Datenschutzkonferenz zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen entnehmen.

DSK: Nationale Benennungspflicht für DSB erhalten

Ziffer 3 des **Entschließungsantrags** des Landes Niedersachsen zur Änderung datenschutzrechtlicher Bestimmungen vom 2. April 2019 enthält folgende Forderung:

"Der Bundesrat fordert eine deutliche Entlastung von kleinen und mittleren Unternehmen von zusätzlichen Bürokratiekosten, die durch das neue Datenschutzrecht entstehen. Gemäß § 38 Abs. 1 S. 1 BDSG haben nichtöffentliche Stellen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Zwar ist diese Regelung nicht neu, sondern an den § 4 f Abs. 1 S. 4 BDSG a. F. angelehnt, sie stellt jedoch eine nationale Besonderheit dar, durch die in Deutschland ansässige Unternehmen gegenüber Unternehmen in anderen Mitgliedsstaaten mit mehr Bürokratie belastet werden.

Der Bundesrat fordert die Bundesregierung daher auf, hier nachzubessern und die in § 38 Abs. 1 S. 1 BDSG genannte Mindestanzahl von zehn Personen deutlich anzuheben. Dies würde insbesondere kleine und mittlere Unternehmen deutlich entlasten, da die Kosten für die Bestellung eines Datenschutzbeauftragten sowie ggfs. dessen Aus- und Fortbildung gerade für diese Unternehmen eine hohe finanzielle aber auch bürokratische Belastung darstellen."

Möglicherweise als Reaktion auf diese nicht ganz neue **Forderung** weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem aktuellen Papier auf die Gefahr hin, dass eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine nicht entlasten, sondern ihnen mittelfristig schade werde.

Die DSK betont, dass sich diese Pflicht seit vielen Jahren bewährt haben und deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten

worden sei. Das bewähre Prinzip der betrieblichen Selbstkontrolle und damit auch die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten.

Ein Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten hätte keine positiven Auswirkungen für die Unternehmen. Ganz im Gegenteil: Bei weiterhin bestehenden Pflichten zur Umsetzung und Gewährleistung datenschutzrechtlicher Anforderungen würden Verantwortliche interne Beraterinnen und Berater zu Fragen des Datenschutzes verlieren.

Die Konferenz spricht sich daher gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Quelle: **Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)**

Anzeige

Datenschutz-Grundlagen

EINFÜHRUNG IN DEN DATENSCHUTZ

Mitarbeiter schulen via E-Learning im TV-Format

Ihre Vorteile:

- Sie kommen Ihrer Unterweisungspflicht gemäß DS-GVO nach und erhalten automatisch eine lückenlose Dokumentation.
- E-Learning ist die kostengünstige Alternative zu Präsenzünterweisungen und reduziert Ihren zeitlichen Aufwand auf ein Minimum.
- Ihre Mitarbeiter führen die Unterweisungen selbstständig und zeitlich unabhängig durch.
- Ihr Logo, Opener und Jingle binden wir kostenlos ein. Auf Wunsch passen wir weitere Elemente Ihrem Corporate Design an.

- Die komplexen Bestimmungen werden verständlich erklärt. Eine Wissensüberprüfung findet durch interaktive Quizfolgen statt.
- Die Schulung hat den Charakter einer Magazinsendung und wurde in einem Fernsehstudio aufgenommen. Unsere Moderatorin führt Sie methodisch durch die Themen.

Die Schulung richtet sich an Mitarbeiter. Eine Schulung für Führungskräfte ist ebenfalls erhältlich. Beide Schulungen auch in englischer Sprache.



Einblicke ins E-Learning-Tool finden Sie **hier**.

Weitere Details finden Sie **hier**.



DATAKONTEXT GmbH · Augustinusstraße 9d · 50226 Frechen · Tel.: 02234/98949-30 · Fax: 02234/98949-32
Internet: www.datakontext.com · E-Mail: kundenservice@datakontext.com

Europäischer Datenschutzausschuss konkretisiert die Vertragserfüllung als Erlaubnistatbestand

Am 10.04.2019 hat der Europäische Datenschutzausschuss (EDSA) seine "**Leitlinien zur Verarbeitung personenbezogener Daten auf Grundlage des Art. 6 Abs. 1 b DS-GVO im Kontext von Online-Dienstleistungen**" ausformuliert.

Art. 6 Abs. 1 b DS-GVO legitimiert die Verarbeitung personenbezogener Daten, soweit sie zur Vertragserfüllung erforderlich ist. Die neu formulierten Leitlinien konkretisieren und schränken diesen Grundsatz insoweit, dass es zur Beurteilung dessen, ob eine Datenverarbeitung zur Vertragserfüllung erforderlich ist, nicht allein darauf ankommt, was im Vertrag vereinbart wurde. Unter Berücksichtigung der in Art. 5 DS-GVO niedergelegten Datenschutzgrundsätze wie Sparsamkeit, Fairness und Transparenz ist nach den Vorgaben des Europäischen Datenschutzausschusses eine Bewertung vorzunehmen, ob Unternehmen die Verarbeitung von Daten der Nutzerinnen und Nutzer auf die Rechtsgrundlage "Vertragserfüllung" stützen können.

Beispielsweise kann eine Datenverarbeitung für Zwecke der personenbezogenen Onlinewerbung danach grundsätzlich nicht auf die Rechtsgrundlage "Vertragserfüllung" gestützt werden. Interessierte Stellen werden die Möglichkeit erhalten das Papier im Rahmen einer öffentlichen Konsultation kommentieren zu können.

Ob die Erforderlichkeit tatsächlich schon dann bejaht werden kann, wenn diese im Rahmen einer Klausel vereinbart wurde oder ob die Erforderlichkeit nicht erst dann angenommen werden kann, wenn die Verarbeitung für die Erfüllung eines Vertrages oder für die Vertragsanbahnung objektiv als erforderlich betrachtet werden muss, ist eine **praxisrelevante Frage**. Ob das Papier am Ende in dieser Hinsicht mehr Rechtssicherheit bringen wird, bleibt abzuwarten. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Ulrich Kelber*, **begrüßt** die Annahme der Leitlinien ausdrücklich.

Das Papier kann in den nächsten Wochen von interessierten Stellen im Rahmen einer öffentlichen Konsultation kommentiert werden.

DS-GVO verunsichert Bildjournalisten

Der Deutsche Journalisten-Verband (DJV) stellt die Ergebnisse seiner jüngsten Umfrage zum Thema "**Fotofreiheit/DS-GVO**" vor. Die Umfrage beschäftigt sich u.a. mit der Frage, welche praktischen Auswirkungen die DS-GVO auf die Arbeit der Bildjournalistinnen und – Journalisten hat.

Von den 200 Teilnehmern an der Umfrage bezeichnen 70 Prozent die Auswirkungen der DS-GVO als negativ. 59 Prozent gaben an: "Durch die DS-GVO ist die Erstellung von Fotos/Filmen zu bürokratisch geworden." Für jeden zweiten Bildjournalisten hat die neue Gesetzgebung zu Umsatzeinbußen geführt. Um den strengen Anforderungen an Datenschutz und Persönlichkeitsrechte zu entgehen, haben sich manche Bildjournalisten darauf verlegt, Personen verfremdet, verpixelt oder von hinten zu fotografieren.

Die zentralen Aussagen fasst der DJV wie folgt zusammen:

- 70 Prozent der Befragten sehen die DS-GVO als negativ bzw. sehr negativ für den Fotojournalismus bzw. die Fotografie an.

- Über die Hälfte der Befragten berichtet, dass sich ihre Arbeitssituation durch die DS-GVO verschlechtert hat und auch zu bürokratisch geworden ist.
- Fast zwei Drittel wählen wegen der DS-GVO andere Fotomotive aus, fotografieren beispielsweise Personen eher von hinten.
- Fast zwei Drittel der Befragten sehen die Qualität der Fotoaufnahmen als gefährdet an, ein Drittel dieses Personenkreises sieht sogar sehr starke Qualitätsverluste.
- Rund 80 Prozent der Befragten arbeiten neuerdings mit einem mulmigen oder sogar schlechten Bauchgefühl, da sie DS-GVO-Risiken befürchten.
- Über zwei Drittel der Befragten fordern, dass die Geltung des Kunsturhebergesetzes in allen Bereichen der Fotografie klar geregelt werden sollten.

Quelle: Deutscher Journalisten-Verband

EuGH prüft Klagebefugnis von Verbraucherverbänden

Der Bundesgerichtshof (BGH) hat ein Verfahren des Bundesverbands der Verbraucherzentralen und Verbraucherverbände (vzbv) gegen Facebook wegen Verstößen gegen Datenschutzrecht ausgesetzt. Das Karlsruher Gericht will auf eine Entscheidung des Europäischen Gerichtshofs (EuGH) warten. Dieser muss noch über ein Vorabentscheidungsverfahren zur Klagebefugnis bei Datenschutzverstößen entscheiden, das ihm vom Oberlandesgericht (OLG) Düsseldorf vorgelegt wurde.

Vorlagefragen des OLG Düsseldorf zur Klagebefugnis von Verbänden

Das OLG Düsseldorf hat dem EuGH in einem Verfahren, in dem es um den "Gefällt mir"-Button von Facebook geht, mehrere Fragen gestellt. Geklärt werden soll dabei die Vereinbarkeit der Art. 22 bis 24 der EG-Datenschutz-Richtlinie mit einer nationalen Regelung zur Rechtsdurchsetzung. Nach § 8 Abs. 3 Nr. 3 UWG sind in Deutschland gemeinnützige Verbände zur Wahrung der Interessen der Verbraucher ermächtigt, im Falle einer Verletzung von Datenschutzvorschriften gegen den Verletzer vorzugehen. Diese Frage ist auch im Rechtsstreit vor dem BGH entscheidungserheblich und nicht zweifelsfrei zu beantworten. Möglicherweise lässt die inzwischen von der Datenschutz-Grundverordnung (DS-GVO) ersetzte EG-Datenschutz-Richtlinie eine Verfolgung von Verstößen allein durch die Datenschutzbehörden und die Betroffenen und nicht durch Verbände zu.

Rechtsstreit vor dem BGH

Auch vor dem BGH geht es um einen Rechtsstreit mit Facebook. Auf der Internetplattform dieses Netzwerks befindet sich ein "App-Zentrum", in dem Facebook den Nutzern kostenlos Online-Spiele anderer Anbieter zugänglich macht. Im November 2012 wurden in diesem App-Zentrum mehrere Spiele angeboten, bei denen unter dem Button "Sofort spielen" folgende Hinweise zu lesen waren: "Durch das Anklicken von „Spiel spielen“ oben erhält diese Anwendung: Deine allgemeinen Informationen, Deine Mail-Adresse, Über Dich, Deine Statusmeldungen. Diese Anwendung darf in deinem Namen posten, einschließlich dein Punktestand und mehr."

Mehr auf DataAgenda

Anzeige

Seminartipp

GDD-Forum – Ihr Dialog mit der Datenschutzaufsicht

26.06.2019 | Hannover

Die Umsetzung des neuen Datenschutzrechts löst immer noch viele Praxisfragen aus. Auf diesem GDD-Forum geben Leiter der Aufsichtsbehörden Antworten. Gegliedert in vier thematische Blöcke werden Datenschutzfragen diskutiert und erörtert. Gestalten Sie das Forum mit: Reichen Sie Ihre persönlichen Fragen ein!

Diskutieren
Sie Ihre Fragen
mit Leitern der
Aufsichtsbe-
hörden!

Nutzen Sie diese einmalige Chance und melden
Sie sich direkt an: www.datakontext.com



DATAKONTEXT GmbH · Augustinusstraße 9d · 50226 Frechen · Tel.: 02234/98949-40 · Fax: 02234/98949-44
Internet: www.datakontext.com · E-Mail: tagungen@datakontext.com



Personalüberlassung als Auftragsverarbeitung?

Frage des GDD-Erfa-Kreises Coburg :

Ein Unternehmen steht mit einem Personaldienstleister in einem vertraglichen Verhältnis, d.h. es werden regelmäßig Mitarbeiter des Personaldienstleisters bei dem Unternehmen eingesetzt; teilweise erfolgt dies nur kurzzeitig für spezielle Projekte, teilweise aber auch über einen längeren Zeitraum hinweg. Im Rahmen der Erbringung der Arbeitsleistung für das Unternehmen haben die Mitarbeiter des Personaldienstleisters auch Zugriffsmöglichkeiten auf personenbezogene Daten des Unternehmens. Die Tätigkeit selbst liegt bei manchen der überlassenen Mitarbeiter in der Erbringung von IT- und Wartungstätigkeiten auf dem System des Unternehmens. Ist in dieser Konstellation ein Auftragsverhältnis im Sinne des Art. 28 DS-GVO zu sehen? Sofern dies verneint wird und kein AVV mit dem Personaldienstleister zu schließen ist, was ist dann aus datenschutzrechtlicher Sicht zu tun? (...)

Antwort des BayLDA:

Wir sehen hier bei der Personalüberlassung keinen Sachverhalt einer Auftragsverarbeitung, sondern im Schwerpunkt eine Zurverfügungstellung von (weiteren) Arbeitskräften, die beim "Einsatz-Unternehmen" wie eigene Mitarbeiter zu sehen und dementsprechend zu befehlen bzw. zu verpflichten sind. Siehe dazu auch das Kurzpapier Nr. 19 der DSK unter https://www.ida.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaefigte.pdf, dort insbesondere auf Seite 2, "Wer muss verpflichtet werden", mit dem Beispiel von Leiharbeitern. Eine Verpflichtung durch den Personaldienstleister ist unzureichend, weil es auf die Gegebenheiten beim "Einsatz-Unternehmen" ankommt (Unterschiede bei Bank, Versicherung, Produktionsbetrieb von Gesundheitsprodukten, usw.). Der Personaldienstleister ist kein datenschutzrechtlicher Subunternehmer, weil er mit den Daten, die die ausgeliehenen Personen beim "Einsatz-Unternehmen" verarbeiten, nichts zu tun hat.

Forschungsbericht: Sanktionen der DS-GVO

Im Forum Privatheit setzen sich Expertinnen und Experten aus sieben wissenschaftlichen Institutionen interdisziplinär, kritisch und unabhängig mit Fragestellungen zum Schutz der Privatheit auseinander. Zu den neuen Veröffentlichungen des Verbunds gehört ein Forschungsbericht mit dem Titel "Das Sanktionsregime der Datenschutz- Grundverordnung – Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden".

Die Forscherinnen und Forscher kommen darin zum Schluss, dass Aufsichtsbehörden ihrer Aufgabe nur dann effektiv nachkommen können, wenn diese hinreichend mit personellen und finanziellen Ressourcen ausgestattet werden, um bei Datenschutzverstößen "abschreckende" Maßnahmen zu ergreifen und Bußgelder auch vor Gericht durchzusetzen. Insbesondere sei es erforderlich, die Aufsichtsbehörden im

Bereich der Rechtsdurchsetzung ausreichend auszustatten. Zusätzlich könnte erwogen werden, verhängte Geldbußen nicht wie bisher in den Haushalt der Bundesländer, sondern unbeschränkt und ohne Bedingungen direkt in den Haushalt der Aufsichtsbehörden fließen zu lassen. Der Forschungsbericht beschäftigt sich auch mit den übrigen Abhilfebefugnissen der Aufsichtsbehörden und arbeitet die Auswirkungen der Sanktion auf die Datenschutzpraxis aus.

Die Autoren weisen darauf hin, dass die Ausarbeitung nur ein grobes und vorläufiges Bild vom Sanktionsregime im Datenschutz zeigen kann, da es sich zunächst um eine erste Momentaufnahme in dem frühen Stadium nach Wirksamwerden der DS-GVO handelt.

Quelle: [forum privatheit](#)

Aufsichtsbehörde gibt Antworten zur Zulässigkeit von Cookies und Tracking

In ihrem Positionspapier "**Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018**" nahm die Datenschutz-Konferenz zu der Frage Stellung, ob wegen des Anwendungsvorrangs der DS-GVO die datenschutzrechtlichen Regelungen des TMG nach dem 25.05.2018 weiterhin anwendbar sein werden.

Im Ergebnis wurde im Positionspapier festgestellt, dass der Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und der Erstellung von Nutzerprofilen dienen, einer vorherigen Einwilligung bedarf. Das bedeutet, dass eine informierte Einwilligung i. S. der DS-GVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Der LfDI Baden-Württemberg hat nun eine **FAQ** veröffentlicht, der die häufigsten Fragen zu dieser Thematik beleuchtet und das Papier

"**Orientierungshilfe für Anbieter von Telemedien**" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sinnvoll ergänzt.

Die FAQs befassen sich mit diesen Fragen:

1. Darf ich Werkzeuge zur Reichweitenanalyse ohne Einwilligung der Nutzer verwenden?
2. Welche Cookies darf ich ohne Einwilligung nutzen?
3. Für welche Cookies und Tracking-Mechanismen brauche ich die Einwilligung der Nutzer?
4. Darf ich Elemente Dritter wie Like und Share Buttons in meine Website einbinden?
5. Was sind die Anforderungen an die informierte, freiwillige, aktive und vorherige Einwilligung?
6. Wie gestalte ich Einwilligungs-Banner?

Kontaktdaten von B2B-Ansprechpartnern: Welche Rechtsgrundlage?

Frage des GDD-Erfa-Kreises Coburg:

Wenn Kontaktdaten von Ansprechpartner der B2B-Kunden verarbeitet werden, wie z. B. die Geschäfts-E-Mail-Adresse und Name, handelt es sich hierbei ja auch um personenbezogene Daten (wenn die E-Mail-Adresse aus Vor- und Nachnamen) besteht. Die Ansprechpartner werden im Rahmen des E-Mailkontaktes bei Datenerhebung bzgl. der Punkte des Art. 13 EU-DS-GVO in einem PDF hingewiesen. Es wird als Rechtsgrundlage Art. 6 Abs. 1 lit. b DS-GVO angegeben, da die Kontaktdaten der Ansprechpartner zur Durchführung des Rechtsgeschäftes mit dem Kunden benötigt werden. Ist die Rechtsgrundlage korrekt?

Antwort des BayLDA:

Artikel 6 Abs. 1 Buchst. b DS-GVO als Rechtsgrundlage ist nur einschlägig, wenn die Vertragsbeziehung zu der natürlichen Person selbst besteht, um deren Daten es geht, also z.B. bei einem Einzelkaufmann oder anderen Einzelpersonen (z.B. Selbständigen).

Wenn die Vertragsbeziehung dagegen z.B. zu einer GmbH besteht, und es werden personenbezogene (Kontakt-)Daten von Mitarbeitern dieser GmbH gespeichert, wäre Artikel 6 Abs. 1 Buchst. f DSGVO die "richtige" Rechtsgrundlage, aufgrund derer der Verantwortliche die (Kontakt-)Daten dieser Mitarbeiter verarbeiten darf, soweit und solange es für die Geschäftsbeziehung zu dem "B2B-Partner" (also z.B. zu der GmbH) erforderlich ist.

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen?
Dann tragen Sie sich unverbindlich und kostenlos ein unter www.datakontext.com/newsletter