Datenschutz
newsbox

Ausgabe
7
2018

DATAKONTEXT

Editorial

Gendatenbanken sind nicht nur für Ahnenforscher ein interessantes Thema, sondern auch für Polizeiermittler. Wenn es der Polizei jedoch gelingt mit Hilfe einer Gendatenbank, die ursprünglich nicht für Ermittlungsbehörden konzipiert war, einen Serienmörder zu fassen, wird dem Datenschützer wieder einmal bewusst, dass in seiner Brust zwei Seelen wohnen. Solch „Faust´schen Irritationen" der Gefühlswelt unterliegen Polizeibehörden meist nicht.
Der Zweck heiligt aber wohl nicht immer die Mittel. Die Grenze scheint erreicht zu sein, wenn Fußball-Fans ohne Ihr Wissen missbraucht werden, mit ihren Smartphone unlizenzierte Übertragungen von Fußballspielen zu enttarnen.
Und auch im eigenen Refugium kann sich die Hardware gegen den Nutzer wenden. Nutzer werden dann zu Opfern häuslicher Gewalt, wenn sich die IoT-Geräte gegen den Nutzer verbünden und diese terrorisieren.
Wenn man bedenkt, dass im Jahre 2020 mehr als 30 Milliarden Geräte jeglicher Art vernetzt sein und zudem meist remote gesteuert werden können, ist es mehr als wahrscheinlich, dass Fälle dieser Art zunehmen werden.
Auch ohne einen Hang zu Dystopien liegt die Befürchtung nahe, dass bereits vorhandene Diskriminierungen ohne eine angemessene Kontrolle von Algorithmen, bzw. zur Gesichtserkennung, eher erstarken dürften. In dem hier beschriebenen Fall liegt die Fehlerquote der Gesichtserkennung bei 98 % - vor allem dann, wenn der Betroffene nicht weiß und männlich ist.
Die Meldung, dass Lehrer Zeugnisse „wegen des Datenschutzes" nun per Hand schreiben müssen, verblasst in Anbetracht der obigen Szenarien doch eher zu einer Lappalie, findet 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

Umgang mit Bildern und Fotografien in der katholischen Kirche

Die Diözesandatenschutzbeauftragten der katholischen Kirche treffen sich in der Regel einmal im Jahr an wechselnden Orten zu gemeinsamen Beratungen über aktuelle Themen und gemeinsame Anliegen aus dem Bereich des kirchlichen Datenschutzes.
Sie unterstützen sich so gegenseitig in der Wahrnehmung ihrer Aufgaben und geben gemeinsame Empfehlungen heraus.
Das Gesetz über den Kirchlichen Datenschutz (KDG) erwartet, dass die kirchlichen Aufsichtsbehörden untereinander zusammenarbeiten. Hierdurch soll eine möglichst einheitliche Anwendung der Datenschutzbestimmungen gefördert werden. Vor diesem Hintergrund haben sich die Diözesandatenschutzbeauftragten zur „Konferenz der Diözesandatenschutzbeauftragten" zusammengeschlossen. Die Grundlagen für ihre Zusammenarbeit sind in der „Geschäftsordnung der Konferenz der Datenschutzbeauftragten der katholischen Kirche Deutschlands" festgelegt.
Die DS-GVO hat insbesondere unter Journalisten, Kameraleuten und Fotografen zu einer gewissen Rechtsunsicherheit geführt. Die Fragen konzentrieren sich darauf, welche Änderungen mit Wirksamwerden der DS-GVO (25. Mai 2018) bzgl. der Bilder von Personen gelten und in wie fern die bekannten Normen des KUG dadurch verdrängt werden. Auf Grund dieser vorherrschenden Unsicherheit gab es bereits einige Anstrengungen hier mehr Klarheit zu verschaffen.
Diese entstandene Verunsicherung hat auch die Konferenz der Diözesandatenschutzbeauftragten zum Anlass genommen, um die rechtlichen Fragen rund um das Thema (neu) zu beleuchten.
Mit dem Inkrafttreten des neuen Gesetzes über den Kirchlichen Datenschutz (KDG) seien die Anforderungen an die Zulässigkeit des Fotografierens bei kirchlichen Veranstaltungen und Ereignissen erheblich angestiegen. Entgegen aller Befürchtungen ist es aber auch nach dem KDG nach wie vor möglich, bei diesen Anlässen zu fotografieren, ohne dass von jedem Einzelnen eine entsprechende Einwilligungserklärung nachzuweisen ist, so die Konferenz der Diözesandatenschutzbeauftragten. Das Fotografieren im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten unterliege dabei nicht den Vorgaben des KDG. Etwas anders gelte aber, wenn die Verarbeitung im Rahmen der Tätigkeit eines Verantwortlichen einer Dienststelle erfolgt.
In der Regel würden beim Fotografieren von Menschen dann personenbezogene Daten erhoben, wenn die Bilder digital (§2 Abs. 1 KDG) im Sinn einer automatisierten Verarbeitung aufgenommen werden und zur Identifikation des Aufgenommenen geeignet sind. Die Verarbeitung personenbezogener Daten sei aber nur unter bestimmten Voraussetzungen datenschutzrechtlich zulässig. In Übereinstimmung mit der DS-GVO gelte auch im KDG weiterhin das Verbot mit Erlaubnisvorbehalt, welches besagt, dass eine Verarbeitung personenbezogener Daten generell nur durch eine Rechtfertigung möglich ist. Das heißt, Bildaufnahmen sind zunächst nach § 6 Abs. 1 KDG verboten, wenn sie nicht auf eine Rechtfertigung gestützt werden können - dies kann entweder eine gesetzliche Grundlage oder eine Einwilligung des Betroffenen in die Verarbeitung sein.

Quelle: Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.

LfD Niedersachsen überprüft Umsetzung der DS-GVO

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD), Barbara Thiel möchte prüfen, wie gut sich die niedersächsischen Unternehmen bisher auf die seit dem 25. Mai geltende Datenschutzgrundverordnung (DS-GVO) eingestellt haben. In einer branchenübergreifenden Querschnittsprüfung schreibt Thiels Behörde in diesen Tagen 50 Unternehmen unterschiedlicher Größe an, die Fragen zu zehn Bereichen des Datenschutzes beantworten sollen.
Den Fragebogen der LfD erhalten zunächst 20 große und 30 mittelgroße Unternehmen aus verschiedenen Branchen, die ihren Hauptsitz in Niedersachsen haben. Bis zum November werden die Mitarbeiterinnen und Mitarbeiter die Antworten auswerten und anschließend bei ausgewählten Unternehmen Vor-Ort-Termine wahrnehmen. Der Abschlussbericht der Querschnittsprüfung soll dann im Mai 2019 vorliegen. Die LfD erhofft sich von dieser bisher größten Prüfung seit Bestehen der Aufsichtsbehörde auch Hinweise für ihre zukünftige Arbeit. So könnten sich zum Beispiel Schwerpunktprüfungen in bestimmten Branchen anschließen. Außerdem erwartet die Behörde Anhaltspunkte dafür, wo noch besonders viel Beratungs- und Aufklärungsbedarf besteht. Als Konsequenz daraus könnten beispielsweise neue Orientierungshilfen erarbeitet werden.

Quelle: Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD)

Orientierungshilfe: Wie erfülle ich als Verantwortlicher meine Informationspflichten?

Die Einführung der Datenschutz-Grundverordnung geht mit einer bewussten Stärkung der Betroffenenrechte einher. „Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen“ heißt es daher ausdrücklich in Erwägungsgrund (ErwGr) Nr. 11.
Hauptpfeiler der neuen Betroffenenrechte sind neben dem strengeren Haftungsregime und den neu eingeführten Einzelansprüchen vor allem die ausgeweiteten Transparenzpflichten bei der Datenverarbeitung. Art. 13 DS-GVO widmet sich den Informationspflichten bei der Direkterhebung, Art. 14 ist das Pendant bei Erhebung von Daten bei Dritten. Die betroffene Person soll die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erhalten (Art. 12 Abs. 1 Satz 1 DS-GVO) und dies stets unentgeltlich (Art. 12 Abs. 5).
Am 11. April 2018 verabschiedete die Artikel-29-Datenschutzgruppe ihr WP 260 zu den Transparenzregeln der Datenschutz-Grundverordnung (DS-GVO).

Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmevorschriften greifen. Die Datenschutzkonferenz hat in Form des Kurzpapiers Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“ bereits erste weitergehende Ausführungen zu diesem Thema veröffentlicht.

Aktuell hat auch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA Brandenburg) eine Orientierungshilfe mit dem Titel „Wie erfülle ich als Verantwortlicher meine Informationspflichten? Rechtliche Anforderungen unter der DS-GVO https://www.lda.brandenburg.de/media_fast/4055/Infoblatt_Informationspflichten.pdf“ veröffentlicht. Darin geht die LDA Brandenburg folgenden Fragen nach:

- 1. Was muss ich als Verantwortlicher tun, um die Informationspflichten aus Art. 13 und 14 Datenschutz-Grundverordnung (DS-GVO) zu erfüllen?
- 2. Muss ich die betroffene Person schriftlich informieren oder reicht ein Verweis auf meine Webseite, auf der ich die Informationen bereitstelle?
- 3. Muss ich nachweisen, dass ich die Informationspflichten erfüllt habe?
- 4. Wer muss die Informationspflichten erfüllen, wenn es sich um gemeinsame Verantwortliche i. S. d. Art. 26 DS-GVO handelt
- 5. Spezielle Fallgruppen

Abgerundet werden die einzelnen Fragen mit passenden Praxisbeispielen.

Quelle: LDA Brandenburg

Zulässigkeit von Fotografien unter der DS-GVO

Die DS-GVO hat insbesondere unter Journalisten, Kameraleuten und Fotografen zu einer gewissen Rechtsunsicherheit geführt. Die Fragen konzentrieren sich darauf, welche Änderungen mit Wirksamwerden der DS-GVO (25. Mai 2018) bzgl. der Bilder von Personen gelten und in wie fern die bekannten Normen des KUG dadurch verdrängt werden. Auf Grund dieser vorherrschenden Unsicherheit gab es bereits einige Anstrengungen hier mehr Klarheit zu verschaffen.
Das Bundesministerium des Innern hat im Rahmen seiner FAQs, die diverse Fragen zum Verständnis der DS-GVO adressieren, auch hierzu Stellung genommen und schildert, unter welchen Voraussetzungen das Anfertigen und Verbreiten personenbezogener Fotografien künftig zulässig ist. Auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat seinen Beitrag zu mehr Klarheit geleistet und setzt sich mit dieser Fragestellung in seinem Vermerk „Rechtliche Bewertung von Fotografien einer unüberschaubaren Anzahl von Menschen nach der DSGVO außerhalb des Journalismus“ auseinander. Last but not least hat auch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg eine Handreichung unter dem Namen „Verarbeitung personenbezogener Daten bei Fotografien Rechtliche Anforderungen unter der DS-GVO“ veröffentlicht. Auch dort seien in den vergangenen Monaten die Anzahl an Nachfragen von Fotografen, Veranstaltern, Bloggern sowie Vertretern aus der Presse und Öffentlichkeitsarbeit zu Personenfotografien unter Geltung der DS-GVO spürbar gestiegen.

Aus der Reihe: „Die Aufsichtsbehörde antwortet...“

Frage 1 des GDD Erfa-Kreises Würzburg:

Zu Art. 15 Abs. 3 S. 3 DS-GVO:
Dieser lautet: Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen (…) Wie kann man das am besten machen, gibt es Empfehlungen / best practices? Bei E-Mails gibt zwei grundsätzliche Probleme: Sichere Datenübermittlung (Verschlüsselung) und Feststellung der Identität des Anfragenden / Betroffenen. Falls ein Unternehmen über ein Kundenportal verfügt, dann kann man darauf aufbauen (Login, Auswahl der Dokumente, etc.), aber ohne …?

Antwort des BayLDA:

Im DSK-Kurzpapier Nr. 6 zum Auskunftsrecht heißt es: „Stellt die betroffene Person ihren Auskunftsantrag elektronisch, ist die Auskunft nach Art. 15 Abs. 3 Satz 2 DS-GVO in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. im PDF-Format).“ Zur sicheren Identifikation und Auskunftszuleitung an die betroffene Person gibt es keine Pauschal-Regeln; hier kommt es auf die Art der Daten (z. B. Gesundheitsdaten bei einem Neurologen einerseits und Adressverlag andererseits) sowie auf die konkrete sonstige Beziehung mit der betroffenen Person an (längere Geschäftsbeziehung oder Neukunde etc.).

Frage 2 des GDD Erfa-Kreises Würzburg:

Hat der Betriebsrat ein Recht in das gesamte Verzeichnis der Verarbeitungstätigkeit des Arbeitgebers einzusehen? Muss der DSB bzw. die verantwortliche Stelle dieses komplett herzeigen oder hat nicht der BRat vielmehr selbst die Aufgabe ein entsprechendes Verzeichnis zu führen, da er ja selbst sog. verantwortliche Stelle ist und der DSB ihn auch nicht kontrollieren darf.

Antwort des BayLDA:

Ob ein Betriebsrat das Recht hat, in das gesamte VVT des Unternehmens einzusehen, beurteilt sich allein nach dem BetrVerfG, wozu wir uns nicht äußern können. Die datenschutzrechtliche Stellung des Betriebsrats in der DS-GVO wird im Moment noch diskutiert. Die vom BAG anhand des BDSG bisher gesehene Sonderstellung wird im Schrifttum unter Geltung der europäischen DS-GVO nunmehr vielfach bezweifelt. Unsere Empfehlung bis auf weiteres: Der Betriebsrat legt nach den Empfehlungen des DSB für seine internen Verarbeitungen personenbezogener Beschäftigtendaten ein VVT an.

Frage 3 des GDD Erfa-Kreises Würzburg:

Nach derzeitiger Rechtslage kann E-Mail-Werbung ohne Einwilligung unter bestimmten Voraussetzungen erfolgen, wenn dabei auch die Wertungen des § 7 Abs. 3 UWG (bzw. künftig Art 16 E-Privacy-VO) beachtet werden (Einzelheiten Anwendungshinweise Düsseldorfer Kreis). Der entsprechende Werbehinweis wurde ja oft in den Vertragsunterlagen durch Umrahmung untergebracht. Im Hinblick auf die EU-DS-GVO und die Informationspflichten gem. Art. 13 EU-DS-GVO interessiert uns, ob für eine transparente Datenverarbeitung nach Ihrer Ansicht auch zwingend über die in Art. 13 Abs. 2 EU-DS-GVO genannten Punkte informiert werden muss oder die Informationen gem. Abs. 1 ausreichen?

Antwort des BayLDA:

Zu den Informationspflichten kann auf das DSK-Kurzpapier Nr. 10, https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf , sowie auf das WP 260 verwiesen werden. Insbesondere das WP 260 stellt unter Nr. 2 klar, dass die jeweiligen Absätze 1 und 2 der Art. 13 und 14 DS-GVO von gleicher Bedeutung sind und die jeweiligen Informationen zur Verfügung gestellt werden müssen. Das WP 260 erkennt allerdings unter Nr. 2.5 auch an, dass insbesondere bei digitalem Kontext mehrstufige Datenschutzinformationen möglich sind, z. B. Kern-Informationen (Verantwortlicher und Zweck der Verarbeitung einschließlich eventueller Empfänger der Daten) als unmittelbare Text-Information, weitere Detail-Informationen sind über einen Link direkt erreichbar.

Frage 4 des GDD Erfa-Kreises Würzburg:

Gem. Art 13 Abs. 1 lit e EU-DS-GVO muss über die Empfänger personenbezogener Daten bzw. über die Kategorien informiert werden. Da Empfänger ja nicht nur Dritte sind, sondern quasi auch ein Auftragsverarbeiter als „verlängerter Arm“ des Verantwortlichen sein kann, interessiert uns, ob wirklich Auftragsverarbeiter auch dazu zählen und wenn ja, ob es dann ausreicht im Hinblick auf die „Kategorien“ von Empfängern diese lediglich pauschal in ihrer Funktion zu benennen? Bei über 100 Dienstleister könnte dies sonst sehr unübersichtlich werden.

Antwort des BayLDA:

Wegen der Informationspflichten allgemein siehe zu Frage 3 (oben). Bei eingesetzten Auftragsverarbeitern reicht regelmäßig die Angabe von Kategorien.

EuGH: Zeugen Jehovas müssen Datenschutz einhalten

Eine Religionsgemeinschaft wie die der Zeugen Jehovas ist gemeinsam mit ihren als Verkündiger tätigen Mitgliedern für die Verarbeitung der personenbezogenen Daten verantwortlich, die im Rahmen einer von Tür zu Tür durchgeführten Verkündigungstätigkeit erhoben werden. Die im Rahmen einer solchen Tätigkeit erfolgenden Verarbeitungen personenbezogener Daten müssen mit den unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten im Einklang stehen, so der EuGH in seiner Entscheidung vom 10.07.2018 (Urteil in der Rechtssache C-25/17 Tietosuojavaltuutettu / Jehovan todistajat – uskonnollinen yhdyskunta).
In seinem Urteil stellt der Gerichtshof zunächst fest, dass die von den Mitgliedern der Gemeinschaft der Zeugen Jehovas von Tür zu Tür durchgehführte Verkündigungstätigkeit nicht unter die Ausnahmen fällt, die die unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten vorsehen. Insbesondere sei diese Tätigkeit keine ausschließlich persönliche oder familiäre Tätigkeit, für die diese Vorschriften nicht gelten. Der Umstand, dass die Verkündigungstätigkeit von Tür zu Tür durch das in Art. 10 Abs. 1 der Charta der Grundrechte der EU verankerte Grundrecht auf Gewissens- und Religionsfreiheit geschützt ist, verleihe ihr keinen ausschließlich persönlichen oder familiären Charakter, da sie über die private Sphäre eines als Verkündiger tätigen Mitglieds einer Religionsgemeinschaft hinausgehe. Sodann weist der Gerichtshof einschränkend darauf hin, dass die unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten nur dann auf die manuelle Verarbeitung von Daten anwendbar sind, wenn diese Daten in einer Datei gespeichert sind oder gespeichert werden sollen. Insoweit gelangt der Gerichtshof zu dem Ergebnis, dass der Begriff „Datei" jede Sammlung personenbezogener Daten, die im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erhoben wurden und zu denen Namen und Adressen sowie weitere Informationen über die aufgesuchten Personen gehören, umfasst, sofern diese Daten nach bestimmten Kriterien so strukturiert sind, dass sie in der Praxis zur späteren Verwendung leicht wiederauffindbar sind. Um unter diesen Begriff zu fallen, muss eine solche Sammlung nicht aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen bestehen.
Zu der Frage, wer als für die Verarbeitung der personenbezogenen Daten Verantwortlicher angesehen werden kann, weist der Gerichtshof darauf hin, dass der Begriff „für die Verarbeitung Verantwortlicher" mehrere an dieser Verarbeitung beteiligte Akteure betreffen kann, wobei dann jeder von ihnen den unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten unterliegt. Diese Akteure können in verschiedenen Phasen und in unterschiedlichem Ausmaß in die Verarbeitung einbezogen sein, so dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist. Die gemeinsame Verantwortlichkeit mehrerer Akteure setze nicht voraus, dass jeder von ihnen Zugang zu den personenbezogenen Daten habe.
Der Gerichtshof gelangt zu dem Schluss, dass nach den unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitung personenbezogener Daten angesehen werden kann, die durch diese Mitglieder im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgt, die von dieser Gemeinschaft organisiert und koordiniert wird und zu der sie ermuntert, ohne dass es hierfür erforderlich wäre, dass die Gemeinschaft Zugriff auf die Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu dieser Datenverarbeitung gegeben hat.

Quelle: Gerichtshof der Europäischen Union

GDD vergibt Wissenschaftspreis im Datenschutz und in der Datensicherheit

In diesem Jahr vergibt die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. erneut einen Wissenschaftspreis für herausragende wissenschaftliche Arbeiten in den Bereichen Datenschutz und Datensicherheit. Der Preis beträgt 5.000,00 €. Der Preis kann auch zwischen mehreren Arbeiten geteilt werden. Der Preis soll bevorzugt an Nachwuchswissenschaftler vergeben werden. Es sollen fertiggestellte oder in der Fertigstellung befindliche Abschlussarbeiten oder Doktorarbeiten ausgezeichnet werden. In Betracht kommen neben Arbeiten aus den Rechtswissenschaften, Wirtschaftswissenschaften und der Informatik auch aus anderen Wissenschaftsdisziplinen, in denen Fragen aus den Bereichen Datenschutz und Datensicherheit behandelt werden. Voraussetzung für die Vergabe des Wissenschaftspreises ist die Erfüllung der wissenschaftlichen Exzellenzkriterien.
Die Arbeiten müssen mit Befürwortung des betreuenden Hochschullehrers bei der GDD-Geschäftsstelle bis zum 31. Juli 2018 eingereicht werden.
Nähere Informationen zum Wissenschaftspreis stehen als PDF-Datei und Word-Dokument als Download zur Verfügung.

Aus der Reihe: „Die Aufsichtsbehörde antwortet...“

Frage 1 des GDD Erfa-Kreises Würzburg:
Unternehmen (A) betreibt eine Online-Plattform, die es z. B. Handwerkerfirmen (B) ermöglicht, per „Chatfunktion“ mit potentiellen Arbeitsmateriallieferanten (C) in Verbindung zu treten. Die Chats verlaufen grundsätzlich anonym, erst wenn man sich handelseinig ist, werden Kontaktdaten ausgetauscht. C wird hierbei regelmäßig Kontaktdaten seiner Mitarbeiter an B zur weiteren Kontaktaufnahme im Chat bekannt geben.
Frage 1: Liegt in dieser Konstellation ein ADV-Verhältnis zwischen A und C vor? A betreibt keine zielgerichtete Auftragsverarbeitung für C, sondern bietet den Chatdienst für eigene Zwecke (Bereitstellung der Plattform, C muss sich hierfür kostenpflichtig registrieren) an. A verarbeitet die im Chat bekannt gegebenen Daten von C auch nicht weiter, die Administratoren von A können im Falle von Wartung des Systems etc. allerdings die Daten einsehen.

Antwort des BayLDA:
Wir sehen hier keine nach § 11 Abs. 2 BDSG bzw. Art. 28 Abs. 3 DS-GVO regelungsbedürftige ADV, denn hier spricht viel dafür, die per Plattform angebotene Chatfunktion als Telekommunikationsdienst mit den TKG-Datenschutzregeln als Rahmenbedingungen anzusehen.

Frage 2 des GDD Erfa-Kreises Würzburg:
Ein Unternehmen betreibt Werbemaßnahmen und hat hierbei nicht lückenlos die für den Werbekanal erforderlichen Einwilligungen eingeholt. Bei der durchgeführten Werbung handelt es sich daher in jedem Falle um einen Verstoß gegen das UWG, welches auch sanktioniert werden kann. Besteht darüber hinaus die Möglichkeit, dass auch seitens der Aufsichtsbehörde ein Bußgeldverfahren aufgrund des Verstoßes gegen Art. 6 Abs. 1 a) EU-DS-GVO (mangelnde Einholung einer Einwilligung) eingeleitet wird oder sind in diesem Falle die Regelungen des UWG lex specialis?

Antwort des BayLDA:
Eine unzulässige Verarbeitung personenbezogener Daten für werbliche Zwecke, z. B. Telefonwerbung ohne vorherige Einwilligung, kann unabhängig von eventuellen UWG-Verfahren von den Datenschutz-Aufsichtsbehörden mit einem Bußgeldverfahren verfolgt werden.

Verpflichtung auf das Datengeheimnis

Aus der Reihe: „Die Aufsichtsbehörde antwortet...“

Frage des GDD Erfa-Kreises Würzburg:

Die Verpflichtung auf das Datengeheimnis ist zwar nicht explizit in der EU-DS-GVO genannt und im BDSG-neu nur für Behörden, allerdings sollen die Unternehmen aus eigenen Interesse ja weiterhin die Mitarbeiter darauf verpflichten. Bei dem Muster nach dem BDSG wurden die Bußgeld-Paragraphen immer angehängt. Da die EU-DS-GVO aber keine Bußgelder gegenüber den Mitarbeitern enthält, fragen wir uns, ob wir diese dann komplett weglassen oder die vom BDSG-neu heranziehen? Was empfehlen Sie?

Antwort des BayLDA:

Zur Erläuterungen für eine Verpflichtung von Beschäftigten unter Geltung der DS-GVO verweisen wir auf unser Info-Blatt „Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ unter https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf.

Dass Geldbußen nach der DS-GVO nur gegen Unternehmen verhängt werden können, sehen wir nicht so. Nr. 150 ErwGr. führt im Satz 4 wie folgt aus: „Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen.“

Mindeststandard zur Mitnutzung externer Cloud-Dienste

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher nun einen Mindeststandard zur Mitnutzung externer Cloud-Dienste veröffentlicht. Der nun durch das BSI auf der gesetzlichen Grundlage von § 8 Abs. 1 BSIG veröffentlichte Mindeststandard zur Mitnutzung externer Cloud-Dienste sorgt dafür, dass Entscheidungen im Vorfeld einer Mitnutzung externer Cloud-Dienste einen transparenten Ablauf haben und dadurch ein definiertes Mindestsicherheitsniveau erreicht wird. Gleichzeitig veröffentlicht das BSI umfangreiche Umsetzungshinweise, durch die IT-Verantwortliche, IT-Sicherheitsbeauftragte und IT-Betriebspersonal konkrete Informationen zur korrekten Interpretation und Umsetzung erhalten. Mit der Veröffentlichung setzt das BSI ein weiteres Signal zum Thema Sicherheitsanforderungen auf dem Cloud-Markt. Die im Mindeststandard enthaltenen Anforderungen können auch Behörden der Länder und Kommunen sowie Unternehmen als Leitfaden für die eigene Inanspruchnahme von Cloud-Angeboten dienen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Info-Portal der Stiftung Datenschutz

Die Stiftung Datenschutz wurde 2013 von der Bundesrepublik Deutschland gegründet. Aufgabe der unabhängigen Einrichtung ist die Förderung des Privatsphärenschutzes.
Eine der Aufgaben der Bundesstiftung ist es, die Fähigkeiten der Bevölkerung zum Schutz der eigenen Daten durch Aufklärung und Bildung zu stärken. Mehr Wissen über die konkreten Möglichkeiten eines vorsichtigen Umgangs mit persönlichen Informationen soll dazu geschaffen werden. Das Inkrafttreten der DS-GVO kann als eine Art Zäsur betrachtet werden, was insbesondere Literatur, Handlungsempfehlungen, Orientierungshilfen und aufsichtsbehördlichen Arbeitspapiere angeht.
Viele, auch öffentlich zugängliche Info-Materialien, sind mit Wirksamwerden der DS-GVO zur Makulatur geworden. In den letzten Jahren hat es jedoch unzählige Infos zur Umsetzung der DS-GVO gegeben, die auch frei zugänglich sind. Verbände, Aufsichtsbehörden und sonstige Fachleute haben sehr viele Informationen zum Thema Datenschutz und speziell zur DS-GVO veröffentlicht. Zunehmend wird es schwieriger den Überblick über die zur Verfügung stehenden Materialien zu behalten. Die Stiftung Datenschutz hat die zahlreichen frei verfügbaren Informationen aus unterschiedlichen Quellen zusammengetragen, übersichtlich gegliedert und eingeordnet. Das Infoportal besitzt zudem eine brauchbare Suchmaschine mit verschiedenen Filterkriterien, wie bspw. Region, Branche, Kategorie Verfassen etc.

Quelle: Stiftung Datenschutz

Verhältnis von DS-GVO und TMG klärungsbedürftig

Am 26. April 2018 hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ihre Position zur Anwendbarkeit des Telemediengesetzes (TMG) als nationales Gesetz neben der Datenschutz-Grundverordnung (DS-GVO) veröffentlicht. Nach Auffassung der DSK stellt der 4. Abschnitt des TMG keine Umsetzung der ePrivacy-Richtlinie dar und genießt deswegen keinen Anwendungsvorrang als spezialgesetzliche Regelung für die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste auf Grundlage des Art. 95 DS-GVO.

Der Verbraucherzentrale Bundesverband (vzbv) erklärt, dass sie diese Positionsbestimmung generell begrüßt. Jedoch sieht die vzbv punktuell weiteren Klärungsbedarf, wie bspw. zu der Frage, in welchem Verhältnis das deutsche Telemediengesetz (TMG) – und hier insbesondere die „Cookie-Regelungen" des § 15 Absatz 3 TMG – zur DSGVO und zur ePrivacy-Richtlinie stehen und welche Bestimmungen in der Übergangszeit anzuwenden sind.

Der vzbv stimme aber der DSK zu, dass die DSGVO grundsätzlich Vorrang vor dem bestehenden nationalen Recht habe und dementsprechend §§ 12, 13, 15 TMG nicht mehr anwendbar sei. Abschnitt 4 des TMG stelle keine Umsetzung der ePrivacy-Richtlinie dar. Daher bestehe kein Anwendungsvorrang des TMG auf Basis des Artikels 95 DSGVO. Diese Auffassung werde nicht nur von der DSK und von Verbraucherschutzorganisationen vertreten, sondern unter anderem auch von hochrangigen Vertretern der EU-Kommission geteilt

§§ 12, 13, 15 TMG setzten in erster Linie die bisherige Datenschutz-Richtlinie um und werden somit durch die DSGVO verdrängt. Selbst wenn man von einer vollständigen Umsetzung der ePrivacy-Richtlinie im TMG ausgehen würde, wäre fraglich, ob das TMG im betroffenen Bereich einen Anwendungsvorrang genießen würde, so der vzbv. Denn Artikel 95 DSGVO beziehe sich lediglich auf die „Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen". Der Begriff der „elektronischen Kommunikationsdienste" werde in Artikel 2 lit. a) der Rahmenrichtlinie definiert und schließt explizit Dienste aus, „die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben".

Quelle: Verbraucherzentrale Bundesverband (vzbv)

EU-Parlament kritisiert EU-US Privacy Shield

Vom 18. bis 19. September 2017 fand die erste jährliche Überprüfung der Funktionsweise des „EU-US Privacy Shield" in Washington D.C. statt. Diese regelmäßige, gemeinsame Überprüfung durch die Europäische Kommission und die US-Regierung basiert auf der Angemessenheitsentscheidung zum Privacy Shield. Dieser Prozess entstand nach den Vorgaben des Europäischen Gerichtshofs im wegweisenden Schrems-Urteil (C-362/14) zur Safe Harbor-Entscheidung der Kommission.
An dieser Überprüfung hatten sich acht Vertreter, der in der Artikel 29-Datenschutzgruppe versammelten europäischen Datenschutzbehörden beteiligt, darunter zwei Vertreter aus Deutschland, einer davon aus dem Haus der BfDI. Die ausführlichen Ergebnisse der Überprüfung sind in einem Bericht der Artikel 29-Datenschutzgruppe zusammengefasst, der zusammen mit der korrespondierenden Pressemitteilung der Artikel 29-Datenschutzgruppe auf der Website der BfDI abrufbar ist.
Die Artikel 29-Gruppe der europäischen Datenschutzbehörden hatte bereits damals von der EU-Kommission Nachbesserungen am Privacy Shield für die Übermittlung von personenbezogenen Daten in die USA gefordert und hielt es für fraglich, ob Daten von EU-Bürgern in den USA so gut geschützt werden wie in der EU.
Die europäischen Datenschutzbehörden hatten die Europäische Kommission aufgefordert, in Nachverhandlungen mit der US-Regierung entscheidende Verbesserungen des Privacy Shield-Mechanismus zu erzielen. Die Datenschutzbehörden hielten es nach der ersten gemeinsamen Überprüfung des Privacy Shield weiterhin für fraglich, ob das vom Privacy Shield geschaffene Datenschutzniveau in den USA tatsächlich der Sache nach gleichwertig mit dem Datenschutzniveau in der EU ist. Dies hatte der Europäische Gerichtshof (EuGH) im sogenannten Schrems-Urteil gefordert, durch das die Vorgängerregelung Safe Harbor gekippt wurde.
Nun äußert auch das Das EU-Parlament Kritik an dem aktuellen Rechtsrahmen für den Datentransfer in die USA . Der „EU-US-Datenschutzschild" sei unzureichend und weise anhaltende Schwächen bei der Achtung der Grundrechte auf, heißt es in einer Entschließung, den die Abgeordneten am Donnerstag (mit 303 zu 223 Stimmen für eine Entschließung) verabschiedeten. Die EU-Kommission wird aufgefordert, die Datenschutzvereinbarung mit den USA auszusetzen, falls die Vereinigten Staaten den EU-Bürgern bis zum 1. September keinen ausreichenden Schutz personenbezogener Daten garantierten.

Quelle: EU-Parlament

Wi-Fi Alliance führt WPA3 ein

Wi-Fi Alliance ist eine gemeinnützige Organisation, die die Wi-Fi-Technologie fördert und Wi-Fi-Produkte zertifiziert, wenn sie bestimmten Interoperabilitätsstandards entsprechen. Die Aufgabe der Wi-Fi-Alliance ist, die Produkte verschiedener Hersteller auf der Basis des IEEE-802.11-Standards zu zertifizieren und so den Betrieb mit verschiedenen Wireless-Geräten zu gewährleisten. Die Wi-Fi-Alliance umfasst über 300 Unternehmen als Mitglieder
Die Wi-Fi Alliance hat heute, am 26.06.2018 offiziell WPA3, den Wi-Fi-Sicherheitsstandard der nächsten Generation, eingeführt, der alle bekannten Sicherheitslücken und drahtlosen Angriffe, einschließlich der gefährlichen KRACK-Angriffe, zu beseitigen verspricht. Angekündigt wurde der neue Standard bereits Januar 2018.
WPA ist ein Standard zur Authentifizierung von drahtlosen Geräten unter Verwendung des Advanced Encryption Standard (AES) Protokolls und soll verhindern, dass Hacker drahtlos übertragene Daten abhören können. Ende letzten Jahres entdeckten Sicherheitsforscher jedoch einen schwerwiegenden Fehler im aktuellen WPA2-Protokoll, genannt KRACK (Key Reinstallation Attack), der es Angreifern ermöglichte, den WiFi-Netzwerkverkehr abzufangen, zu entschlüsseln und sogar zu manipulieren. Obwohl die meisten Gerätehersteller ihre Geräte gegen KRACK-Angriffe gepatcht haben, beeilte sich die WiFi Alliance ohne große Verzögerung, WPA3 fertigzustellen und zu starten, um die technischen Mängel von WPA2 von Grund auf zu beheben. Details zu den Sicherheitsfunktionen in WPA3 stellt die Wi-Fi Alliance auf dieser Seite bereit.
Nach Angaben der Wi-Fi Alliance ist WPA3 abwärtskompatibel. WPA3 wird auch WPA2 unterstützen, man kann also auch beide Standards gleichzeitig einsetzen, ein Gerät das also nur WPA2 beherrscht, wird sich auch in einem WPA3-WLAN einsetzen lassen.

Quelle: Wi-Fi Alliance