Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 04/2018

Der IT-Ticker 04/2018 informiert Sie über folgende Themen:

Transparenzanforderungen an die Videoüberwachung

Mit Wirksamwerden der DSGVO müssen deren Regelungen auch im Hinblick auf die Videoüberwachung eingehalten werden. Bereits im Januar haben die Datenschutzbehörden im DSK Kurzpapier Nr. 15 Anwendungshinweise zur Videoüberwachung unter der Geltung der DSGVO veröffentlicht.

Neben der Rechtmäßigkeit der Videoüberwachung ist besonderes Augenmerk auf die korrekte Ausschilderung der Videoüberwachung zu legen. In dieser Hinsicht bringt die DSGVO neue Anforderungen – der Umfang der zu erteilenden Informationen wurde durch die Transparenzvorschriften der DSGVO (Art. 12. ff. DSGVO) erheblich erweitert. So muss ab dem 25. Mai 2018 nicht nur über den Umstand der Videoüberwachung und den dafür Verantwortlichen informiert werden, sondern auch die Kontaktdaten des Datenschutzbeauftragten, die Verarbeitungszwecke sowie die Rechtsgrundlage, die Dauer der Speicherung und ein Hinweis auf Zugang zu den weiteren Pflichtinformationen benannt werden.

Aufgrund des Umfangs der zu erteilenden Informationen wird der Hinweis auf die Videoüberwachung künftig im DIN A4-Format zu erfolgen haben. Die Datenschutzkonferenz hat sich insofern auch auf ein Muster-Hinweisschild verständigt.

Praxistipp:
Unternehmen müssen sicherstellen, dass bei einer Videoüberwachung ausreichend transparent auf diese hingewiesen wird. Zwar muss nicht das von den Aufsichtsbehörden bereitgestellte Muster verwendet werden. Es muss jedoch bei Nutzung eines „eigenen“ Hinweisschildes darauf geachtet werden, dass die von den Aufsichtsbehörden geforderten Informationen gut leserlich enthalten sind. Eine intransparente Videoüberwachung verstößt gegen die Regelungen der DSGVO und kann erhebliche Bußgelder nach sich ziehen. Zudem kann die Aufsichtsbehörde das Betreiben der Videoüberwachung (vorübergehend) untersagen.

Franziska Ladiges, Frankfurt/Main

Blockchain vs. DSGVO

„Blockchain“ und „DSGVO“ gehören sicherlich zu den beliebtesten Buzzwords in diesem Jahr. Die Blockchain ist eine Technologie, die nach Auffassung vieler großes Potenzial für die Zukunft hat. Die DSGVO beschäftigt Unternehmen schon jetzt. Bei der Umsetzung der ersten Blockchain-Use-Cases wird daher aktuell auch stets das Thema Datenschutz diskutiert, denn in der Blockchain werden umfangreich Daten verarbeitet.
Das dezentrale Blockchain-Netzwerk lebt von komplexen Verschlüsselungen und der transparenten Verkettung von Transaktionen in einer zeitlichen Abfolge, die dauerhaft gespeichert werden. Daher gilt die Technologie als besonders sicher und vertrauenserweckend. Somit ist es das Wesen der Blockchain, Daten dauerhaft zu speichern. Wie aber kann dies mit dem Grundsatz des Rechtes auf Vergessenwerden in Einklang gebracht werden, das die DSGVO in Artikel 17 regelt?

Findet die DSGVO überhaupt Anwendung?

Zunächst stellt sich die Frage, ob die DSGVO überhaupt anwendbar ist. Die DSGVO ist nur dann anwendbar, wenn personenbezogene Daten verarbeitet werden. Werden Daten anonym verarbeitet, muss die DSGVO nicht beachtet werden. Naheliegend ist daher die Annahme, dass in der Blockchain durch komplexe Verschlüsselungen und Hash-Werte die Daten anonymisiert sind.

In einer sog. Public Blockchain, auf die jedermann zugreifen kann, können Hash-Werte tatsächlich Anonymität bieten, wenn z.B. die Rohdaten nicht bekannt sind. Häufig werden Daten allerdings nur pseudonymisiert verarbeitet, da Rohdaten noch verfügbar sind. Werden Daten pseudonymisiert verarbeitet, sind die Datenschutzgesetze anwendbar. Unter personenbezogenen Daten werden nämlich alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, verstanden. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, u.a. mittels Zuordnung zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung identifiziert werden kann. Eine Pseudonymisierung lässt eine solche Identifizierung regelmäßig zu. Damit muss die DSGVO beachtet werden.

Für zulassungsbeschränkte und sog. Private Blockchains, zu denen nur ein abgegrenzter Teilnehmerkreis Zugang hat, kann durch Vergabe der Nutzerkennung grundsätzlich auf die Person hinter dem vergebenen öffentlichen Schlüssel zurückzuschließen sein. Damit sind bei derartigen Blockchains die Datenschutzgesetze anwendbar.

Wie kann die DSGVO auf die Blockchain angewendet werden?

Wie Blockchain-Anwendungen DSGVO-konform gestaltet werden können, ist derzeit äußerst fraglich. Schon das eingangs erwähnte Problem, wie das Recht auf Vergessenwerden umgesetzt werden soll, scheint derzeit unlösbar. Fraglich ist auch, wie die weiteren Betroffenenrechte geltend gemacht werden können. Wem gegenüber muss das Auskunftsrecht geltend gemacht werden? In welchem Umfang muss der Verantwortliche Auskunft erteilen? Wer ist überhaupt verantwortliche Stelle, d.h. wer entscheidet in der Blockchain über Zwecke und Mittel der Verarbeitung? In der Public Blockchain könnten verantwortliche Stellen evtl. die Betreiber der Nodes (d.h. Teilnehmer, die selbst Transaktionen vornehmen können) sein. In einer zulassungsbeschränkten oder Private Blockchain könnte verantwortliche Stelle evtl. die Organisationseinheit zur Zugangsberechtigung sein. Insoweit muss in Zukunft unbedingt Klarheit geschaffen werden, denn diese Informationen müssen gemäß Artikel 13 bzw. Artikel 14 DSGVO erteilt werden, wenn eine Informationserteilung nicht nach Artikel 14 Abs. 5 lit. b) DSGVO als unverhältnismäßig bewertet werden kann.

Verhindert die DSGVO Blockchain-Projekte?

Nach den aktuellen Gegebenheiten sind Blockchain-Projekte schwer mit der DSGVO zu vereinen, wenn personenbezogene Daten in der Blockchain gespeichert werden. Da der Technologie jedoch großes Potenzial prophezeit wird, ist es nicht unwahrscheinlich, dass die bestehenden Hürden – z.B. durch Gesetzesänderungen – genommen werden. Verschiedene Verbände veröffentlichen bereits Lösungsvorschläge, wie der Datenschutz zukünftig angepasst werden muss, damit die Blockchain-Technologie erfolgreich eingesetzt werden kann.

Yvonne Schäfer, Frankfurt/Main

Schmerzensgeld für Spam-Mails – Wie schmerzhaft ist Werbung wirklich?

Das AG Diez hat sich in einer Entscheidung vom 07.11.2018 (Az.: 8 C 130/18) mit der Frage befasst, ob die unerlaubte Zusendung einer Werbe-E-Mail die Zahlung eines Schmerzensgeldes nach der DSGVO nach sich ziehen kann.
Der Kläger erhielt am 25.05.2018 von der Beklagten eine E-Mail, mit welcher sie im Hinblick auf das Inkrafttreten der DSGVO nach einer Einwilligung zum Newsletter-Bezug fragte. Hierin sah der Kläger eine unrechtmäßige Datenverarbeitung und damit einen Verstoß gegen Art. 6 DSGVO, der ihm einen – verschuldensunabhängigen – Anspruch auf Ersatz seiner materiellen und immateriellen Schäden nach Maßgabe des Art. 82 Abs. 1 DSGVO vermittle.

Die Beklagte erkannte einen Anspruch des Klägers in Höhe von € 50 (nebst Prozesszinsen!) an, woraufhin am 07.09.2018 ein Teilanerkenntnisurteil erging. Der Kläger begehrte in der Folge von der Beklagten jedoch die Zahlung eines weiteren Schmerzensgeldes in Höhe von mindestens € 500.

Die lehnte das Gericht ab. Aus dem Wortlaut des Art. 82 DSGVO gehe bereits eindeutig hervor, dass ein bloßer Verstoß gegen die DSGVO ohne Schadenseintritt nicht zu einer Haftung führe. Zwar sei einerseits eine schwere Verletzung des Persönlichkeitsrechts nicht mehr erforderlich, andererseits sei auch weiterhin nicht für Bagatellverstöße bzw. für jede bloß individuell empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren. Unter Bezugnahme auf die einschlägige Kommentarliteratur führte das Gericht aus, dass ein spürbarer Nachteil beim Betroffenen entstanden sein und es um eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen müsse.

Dies berücksichtigend kam das Gericht zu dem Ergebnis, dass ein Schmerzensgeldanspruch, so er denn überhaupt bestanden habe, jedenfalls mit dem anerkannten Betrag abgegolten sei.

Praxistipp:
Zwar ließ das Gericht die Frage, ob das unerlaubte Zusenden einer Werbe-E-Mail überhaupt einen Schmerzensgeldanspruch begründen kann, ausdrücklich offen. Indes erscheint dies aufgrund des gerichtlichen Hinweises auf die notwendige „spürbare Beeinträchtigung“ als eher abwegig. Hiervon unberührt bleibt jedoch das Risiko der Abmahnung unter Wettbewerbern wegen § 7 UWG in derartigen Fällen.

Maximilian Wegge, München

Die neue Geoblocking-Verordnung – Abbau von Barrieren im grenzüberschreitenden Online-Handel

Mit zwei Verordnungen sagt die Europäische Union (EU) dem Geoblocking den Kampf an.
Bereits letztes Jahr im Sommer verabschiedete die Europäische Union die sog. Portabilitätsverordnung, die die grenzüberschreitende Nutzung von kostenpflichtigen Online-Diensten für Abonnenten (z.B. Film- und Serienstreaming) bei vorübergehendem Aufenthalt in einem anderen EU-Mitgliedstaat ermöglicht (https://www.skwschwarz.de/aktuelles/artikel/artikel-detail/news/online-auf-die-lieblingsserie-zugreifen-endlich-auch-im-urlaub/4/detail/News/). Nun legte sie am 27. Februar 2018 noch einmal für den grenzüberschreitenden Online-Handel mit der Verordnung zum „ungerechtfertigten Geoblocking“ als Erscheinungsform der Diskriminierung von EU-Bürgern (EU 2018/302) nach. Die Verordnung trat bereits am 23. März 2018 in Kraft, findet aber erst ab dem 3. Dezember 2018 Anwendung. Diese Umsetzungsfrist soll insbesondere kleineren Händlern die Möglichkeit zur Anpassung geben.

Was ist Geoblocking?

Als Geoblocking kann man allgemein jede technische Vorrichtungen auf Websites von Dienstleistern oder Warenanbietern bezeichnen, die dazu führt, dass ein Internetnutzer aufgrund seines aktuellen, geographischen Standortes in einem Land (erkennbar durch die sog. IP-Adresse) nicht auf die Angebote einer Website in einem anderen Land zugreifen kann. Versucht er es doch, bekommt er in den meisten Fällen entweder eine Fehlermeldung oder er wird auf eine andere Website des Anbieters, die dem Standort seiner IP-Adresse entspricht, automatisch umgeleitet. Die gängigste Form des Geoblockings ist jedoch die Verweigerung der Lieferung an Kunden in einem anderen Land, gefolgt von der Verweigerung der Annahme von Zahlungen solcher Kunden. Einige Anbieter greifen wiederum auf das sog. Geo-Filtering zurück. Hierbei kann der Internetnutzer zwar auf die Angebote

der ausländischen Website zugreifen. Er erhält aber – ohne es zu merken – andere Bedingungen als die Internetnutzer eines anderen Landes.

Nicht selten steckt hinter einem systematischen Geoblocking die kartellrechtswidrige Absatz-strategie internationaler Unternehmen, die nationalen Märkte aufzuteilen, um unterschiedliche Preise für die gleiche Leistung aufrufen zu können. Diese Realität stellte unlängst auch die Eu-ropäische Kommission im Rahmen einer sog. Sektorenuntersuchung für den grenzüberschrei-tenden Online-Handel fest (Abschlussbericht der Europäischen Kommission über die Sekto-renuntersuchung im elektronischen Handel vom 10.5.2017, Rn. 49 http://ec.europa.eu/competition/antitrust/sector_inquiry_final_report_de.pdf). Allerdings basierten nach den Feststellungen der Kommission die meisten Geoblocking-Maßnahmen in Bezug auf Verbrauchsgüter auf der freiwilligen Entscheidungen von Einzelhändlern, nicht grenzüberschreitend zu verkaufen. Auf diese zielen auch die Vorschriften der Verordnung ab.

Welchen Zweck hat die Verordnung?

Ziel der Verordnung ist die Schaffung eines europäischen, digitalen Binnenmarktes. Die Verordnung soll die grenzüberschreitende Gleichbehandlung von Internetnutzern innerhalb der EU ohne Rücksicht auf Staatsbürgerschaft, Wohnsitz (Niederlassung) oder Standort bewirken. Sie findet aber nicht nur Anwendung auf Verbrauchergeschäfte (B2C), sondern auch eingeschränkt für Geschäfte zwischen Unternehmern (B2B). Erforderlich ist bei diesen aber, dass der Besteller Endkunde ist, d.h. er die bestellte Ware bzw. elektronische Dienstleistung nicht weiterverkauft oder weiterverarbeitet. Diese Einschränkung ist von der EU bewusst gewählt worden, um nicht in B2B-Vertriebsnetze einzugreifen, die auf einer Auswahl der Händler durch den Hersteller/Großlieferanten beruhen, wie dies z.B. bei selektiven Vertriebssystemen oder Alleinvertriebsvereinbarungen der Fall ist. Hier gewährleiste nach Auffassung des EU-Gesetzgebers das Kartellrecht den Schutz des grenzüberschreitenden Handels.

Welche Regelungen enthält die Verordnung für den Online-Handel?

Klarzustellen ist zunächst, dass nicht das Geoblocking allgemein durch die neue Verordnung verboten wird, sondern nur das „ungerechtfertigte Geoblocking“. Geoblocking im Online-Handel bleibt also weiterhin möglich, wenn auch unter sehr engen Voraussetzungen. Eine denkbare Ausnahme besteht, wenn tatsächlich unterschiedliche Markt- oder Rechtsrahmenbedingungen auf nationalen Märkten herrschen (z.B. infolge staatlicher Regulierung) und dadurch Leistungen nicht in gleicher Weise in verschiedenen Mitgliedstaaten angeboten werden können bzw. dürfen. Das Vorliegen solcher Gegebenheiten dürfte aber der Online-Händler, der Geoblocking verwendet, zu beweisen haben.

Die Verordnung gilt für alle Waren und Dienstleistungen die online angeboten werden und nicht vom Anwendungsbereich ausgenommen sind (hierzu unten unter 4.). Sie verbietet im Wesentlichen zwei hintereinander geschaltete Formen des Geblockings:

Eine Sperrung oder Zugangsbehinderungen zum Webshop für Kunden, die sich in einem anderen EU-Mitgliedstaat aufhalten als der Online-Händler. Die Umleitung zur Website (URL) eines anderen EU-Mitgliedstaates kann daher nur mit Zustimmung des Kunden erfolgen. Ein Anbieten von ungleichen Verkaufs-, Liefer- und Zahlungsbedingungen. Allerdings bleiben unterschiedliche, länderspezifische Bedingungen weiterhin zulässig.

Diese Regelungen zwingen einen Online-Anbieter jedoch nicht dazu, jeden EU-Mitgliedstaat zu beliefern, also auch einen, in dem er gar keinen Verkauf anbietet. Bestellt aber ein Kunde aus einem solchen EU-Mitgliedstaat bei dem Online-Anbieter Waren, muss der Online-Händler ihm aber entweder ermöglichen, die Ware abholen zu lassen oder sie in einen EU-Mitgliedstaat zu versenden, den er beliefert.

Worauf oder für wen findet die Verordnung keine Anwendung?

Ausgenommen vom Anwendungsbereich der Verordnung sind lediglich:
- Online-Händler unter EUR 17.500,00 Jahresumsatz (Kleinunternehmer)
- Streaming oder Downloadangebote für urheberrechtlich geschützt Werke wie Musik, Filme, E-Books, Übertragung von Sportereignissen (einige dieser Dienste unterliegen aber der Portabilitätsverordnung)
- Gesundheitsleistungen und soziale Dienste

- Finanzdienstleistungen
- Beförderungsleistungen (Flugzeug, Bahn, Schiff etc.)
- B2B-Geschäfte, bei denen das beziehende Unternehmen nicht selbst Endkunde ist

Was erwartet Unternehmen bei Verstößen?

Verstoßen Online-Anbieter gegen die Bestimmungen der Verordnung, drohen diesen verschiedene Sanktionen. Diese sind von den jeweiligen Mitgliedstaaten autonom festzulegen. Sie müssen wirksam, verhältnismäßig und abschreckend sein. Deutschland hat bisher keine Sanktion- bzw. Bußgeldregelungen erlassen.

Zusätzlich sollen Beschwerdestellen eingerichtet werden, die Verbraucher bei Streitigkeiten mit Anbietern unterstützen. Verbraucherorganisationen können zudem gegen die Online-Händler auf Unterlassung klagen.

Unabhängig davon kann die Verpflichtung eines Online-Händlers seitens eines Hersteller oder Großhändlers, Geoblocking-Maßnahmen zu verwenden, einen Verstoß gegen das Europäische Kartellrecht beinhalten, wenn dadurch unzulässige Gebiets- oder Kundenbeschränkungen generiert oder verfestigt werden. In diesem Fall drohen Online-Händlern und Herstellern/Großhändlern nicht unerhebliche Bußgelder.

Ausblick und Praxistipp
Die Verordnung greift in die Vertriebssteuerung des Einzelhandels ein. Anbieter, die in den Anwendungsbereich der Verordnung fallen, sollten die Zeit bis zum 3. Dezember 2018 nutzen, um zu überprüfen, ob sie Geoblocking oder andere Formen der Diskriminierung innerhalb der EU verwenden. Dies gilt insbesondere für unterschiedliche Verkaufs-, Zahlungs- und Lieferbedingungen bei Bestellungen aus verschiedenen EU-Mitgliedstaaten. Ist dies der Fall, kann eine dementsprechende Ungleichbehandlung nur aufrechterhalten werden, wenn eine sachliche Rechtfertigung hierfür besteht (z.B. abweichende Portokosten). Weiter müssen die Vorausset-zungen geschaffen werden, dass Kunden aus anderen EU-Mitgliedstaaten ihre Bestellungen beim Online-Anbieter abholen können oder diese an eine Lieferadresse in einem belieferten EU-Mitgliedstaat versendet werden können.

Wie groß letztendlich die wirtschaftlichen Auswirkungen der Verordnung sind, bleibt abzuwarten. Am Ende scheitert eine grenzüberschreitende Bestellung nicht selten an den Sprachbarrieren. Denn Online-Händler sind durch die Verordnung nicht gezwungen, ihre Website in einer anderen Sprache zu gestalten, als der des eigenen EU-Mitgliedstaates.

Dr. Philipp Asbach, Hamburg

Berliner Beauftragte für Datenschutz bringt Zündstoff in die Diskussion um Facebook-Fanpages

Als am 5. Juni 2018 der EuGH entschieden hat, dass Betreiber einer Facebook-Fanpage gemeinsam mit Facebook für die Verarbeitung personenbezogener Daten der Besucher der Fanpages datenschutzrechtlich verantwortlich sind (wir berichteten), sind viele Unternehmen aufgeschreckt. Als daraufhin im September 2018 die Datenschutzkonferenz einen Beschluss veröffentlicht hat, welcher sinngemäß aussagt, dass Facebook-Fanpages ohne entsprechende Vereinbarung nicht rechtmäßig betrieben werden können, schlossen viele Unternehmen tatsächlich ihre Fanpages. Als Facebook kurze Zeit später reagierte und eine Vereinbarung zur gemeinsamen Verantwortlichkeit – sog. Page Controller Addendum – zur Verfügung stellte, atmeten viele wieder auf und sahen das Problem als gelöst an.
Seit dem 15. November 2018 versendet nun aber die Berliner Beauftragte für Datenschutz und Informationsfreiheit Anhörungsschreiben. Darin werden 15 Fragen zur datenschutzrechtlichen Mit-Verantwortlichkeit an den Facebook-Fanseiten gestellt. Diese gehen wesentlich weiter in die Details als die Fragen, welche die Datenschutzkonferenz in ihrem Beschluss aus dem September stellte. Unternehmen dürfte es schwer fallen, diese Fragen ohne die Hilfe von Facebook zu beantworten. Allein anhand dieser Fragen lässt sich feststellen, dass die Berliner Behörde wohl weiterhin Zweifel an der Rechtmäßigkeit des Betriebs einer Fanpage hat. In einer parallelen Pressemitteilung heißt es dazu auch:

„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."

Was aber sollen Unternehmen nun tun?

Praxishinweise:
Fanpage-Betreiber sollten nicht in Panik verfallen. Die Vereinbarung des Page Controller Addendum durch Akzeptieren der Nutzungsbedingungen – im Endeffekt einfacher Weiterbetrieb der Fanpage – ist ein erster Schritt, um den Anforderungen der Datenschutzkonferenz nachzukommen. Ferner muss in der eigenen Datenschutzerklärung ein Hinweis auf den Betrieb der Fanpage, die gemeinsame Verantwortlichkeit und den Grobinhalt der Vereinbarung aufgenommen werden. Zwar hat sich Facebook in dem Addendum verpflichtet, den Nutzern den Grobinhalt des Addendums zu Verfügung zu stellen, solange dies jedoch noch nicht der Fall ist, sollten sich Betreiber einer Fanpage entsprechend selbst absichern. Zudem müssen Betreiber einer Fanpage für die eigene Verarbeitung eine Rechtsgrundlage für die Verarbeitung darlegen. Dies dürfte in aller Regel das berechtigte Interesse des Betreibers an Marketing und Auswertung der Marketingaktivitäten sein. Schließlich sollten sich Unternehmen mit den Fragen der Datenschutzkonferenz als auch mit den Fragen der Berliner Behörde befassen und diese im Zweifel beantworten können.

Zwar können auch diese Maßnahmen keinen vollumfänglichen Schutz gewährleisten, aber bis das Bundesverwaltungsgericht abschließend entscheiden hat, sollten keine voreiligen Handlungen vorgenommen werden.

Franziska Ladiges, Frankfurt/Main

Neuer Leitfaden der Medienanstalten – Werbekennzeichnung für Influencer nun ganz einfach?

Die Landesmedienanstalten haben Mitte November 2018 ihren überarbeiteten Leitfaden zur Werbekennzeichnung bei Social-Media-Angeboten veröffentlicht. Der neue Leitfaden ist als „Kennzeichnungsmatrix" mit Unterteilung nach Art der Inhalte sowie der Medien (Videos auf YouTube/Facebook, Text/Bilder auf Instagram/Facebook/Twitter und Blogs) aufgebaut. Er soll Influencern und werbenden Unternehmen Hilfestellung für die korrekte Trennung und Kennzeichnung von Werbung geben. Die wichtigsten Erkenntnisse sind im Folgenden zusammengefasst:

- Die Erwähnung oder Darstellung von Produkten, Marken, Dienstleistungen usw. aufgrund einer Kooperation ist stets als Werbung zu kennzeichnen, unabhängig davon, ob hierfür eine Gegenleistung erfolgte.
- Sofern keine Kooperation mit einem Unternehmen vorliegt, soll es sich in der Regel nicht um Werbung handeln. In diesem Zusammenhang weist der Leitfaden jedoch ausdrücklich auf die jüngsten Fälle aus der Rechtsprechung hin, bei denen die Verlinkung auf kommerzielle Instagram-Accounts von Modefirmen auf einem Instagram-Post als Werbung betrachtet wurde, obwohl die dargestellten Produkte selbst erworben wurden und keine Gegenleistung erfolgte.
- Nach Ansicht der Medienanstalten sind die von Instagram, Facebook und YouTube zur Verfügung gestellten „Branded Content Tools" alleine nicht ausreichend, um den Werbecharakter eines Beitrags zu kennzeichnen. Die zusätzliche Verwendung dieser Tools wird aber durchaus empfohlen.
- Wie schon in der vorherigen Fassung des Leitfadens raten die Landesmedienanstalten weiter von der Verwendung englischsprachiger Begriffe wie „sponsored by", „ad" oder „PR Sample" ab.
- Nach Auffassung der Medienanstalten sind Verlinkungen auf kommerzielle Websites sowie Rabattcodes stets als Werbung zu kennzeichnen. Auch Affiliate Links sollten z.B. mit einem Sternchen-Hinweis kenntlich gemacht und mit einer Erläuterung versehen werden.

Der neue Leitfaden ist vor dem Hintergrund der jüngst ergangenen Gerichtsentscheidungen, insbesondere dem Urteil des LG Berlin vom 24. Mai 2018 (Az. 52 O 101/18), zu sehen. Als Reaktion auf dieses Urteil kennzeichnen seitdem viele Influencer jeden Beitrag als Werbung. Die übersichtlichen Handlungsempfehlungen der Medienanstalten sind daher sehr zu begrüßen, damit die Trennung zwischen werblichen und sonstigen Inhalten auf Social Media nicht vollends verloren geht. Allerdings ist zu beachten, dass es sich bei dem Leitfaden eben nur um Empfehlungen handelt, an welche die Gerichte nicht gebunden sind.

Corinna Sobottka, München

EU-weite Sicherheitszertifizierungen für IT-Produkte

Die EU bekräftigt das Ziel einer Verordnung zur Cybersicherheit. Im Fokus steht dabei auch ein verbesserter Schutz von Geräten im IoT durch Sicherheitszertifizierungen.
Im Oktober 2018 hat der Europäische Rat erneut dazu aufgerufen, Beschlüsse der EU zur Stärkung der IT-Sicherheit zeitnah umzusetzen. Neben der raschen Implementierung der NIS-Richtlinie in den Mitgliedstaaten beabsichtigt die EU insbesondere weiterhin den Erlass einer Verordnung zur Cybersicherheit. Ein Entwurf der Verordnung liegt seit Mai 2018 vor.

Ziel des Verordnungsvorschlages ist neben Ausbau und Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) die Einführung eines EU-weiten Zertifizierungsrahmens für die Cybersicherheit.

Unternehmen der IT-Branche sollen so die Möglichkeit zur EU-weiten Sicherheitszertifizierung ihrer IT-Produkte und Dienste erhalten. Vorgesehen sind dafür aktuell sog. Vertrauenswürdigkeitsstufen „niedrig", „mittel" oder „hoch". IT-Produkte mit Vertrauenswürdigkeitsstufe „niedrig" soll der Hersteller selbst zertifizieren können, für Produkte der Stufen „mittel" oder „hoch" kann die Zertifizierung nur durch eine Konformitätsbewertungsstelle oder die nationale Cybersicherheitszertifizierungsstelle erfolgen. Der aktuelle Entwurf sieht die Zertifizierung als nicht verpflichtend, sondern freiwillig vor.

Die Verordnung zur Cybersicherheit soll im Herbst 2018 inhaltlich finalisiert und bis Anfang 2019 beschlossen werden.

Dr. Daniel Meßmer, München

Freier Datenverkehr in der EU ab 2019

Die Abschaffung nationaler Beschränkungen zur Datenlokalisierung soll grenzüberschreitende Technologien wie Cloud-Dienste und künstliche Intelligenz in der EU stimulieren.
Mit Beschluss vom 09.11.2018 hat der Rat der EU der Verordnung über den freien Verkehr nicht-personenbezogener Daten zugestimmt. Die Verordnung verbietet den Mitgliedstaaten künftig jede Form von Datenlokalisierungsauflagen, also gesetzliche oder behördliche Vorgaben, wonach die Datenverarbeitung nur im Hoheitsgebiet des jeweiligen EU Mitgliedsstaates stattfinden darf.

So sieht etwa § 146 Abs. 2 S. 1 Abgabenordnung (AO) aktuell vor, dass steuerrechtlich relevante Aufzeichnungen grundsätzlich in Deutschland aufbewahrt werden müssen. Eine Speicherung auf einem Server im Ausland ist bislang nur mit Bewilligung der zuständigen Finanzbehörde möglich.

Diese sowie alle weiteren Datenlokalisierungsvorgaben werden durch die Verordnung abgeschafft. Dadurch sollen Datenaktivitäten innerhalb der EU erleichtert und die europäische Datenwirtschaft gestärkt werden.

Die Verordnung tritt sechs Monate nach der nun anstehenden Unterzeichnung durch das EU-Parlament und anschließender Verkündung, also voraussichtlich im Frühjahr 2019 in Kraft.

Praxistipp:
Der so geschaffene, freie Datenverkehr betrifft ausschließlich Daten ohne Personenbezug. Für Daten mit Personenbezug sind auch weiterhin stets die Vorgaben der DSGVO zu beachten.

Dr. Daniel Meßmer, München

Prüfpraxis der Aufsichtsbehörden für Datenschutz am Beispiel der Veröffentlichung von Prüfplänen des Bayerischen Landesamtes für Datenschutzaufsicht

Die Datenschutzgrundverordnung (DSGVO) ist seit dem 25. Mai 2018 unmittelbar geltendes Recht. Sie hat insbesondere aufgrund der erheblich gestiegenen Bußgeldandrohung von bis zu 4 % des weltweit erzielten Vorjahresumsatzes oder € 20 Millionen für große mediale Aufmerksamkeit gesorgt. Nicht zuletzt wegen der vielen ausfüllungsbedürftigen und abstrakten Rechtsbegriffe haben sich neben den unmittelbar Verpflichteten und Rechtsanwendern natürlich zunächst auch die

Aufsichtsbehörden mit der neuen Rechtslage vertraut machen müssen. Dass sich diese „Eingewöhnungsphase“ langsam aber sicher einem Ende zubewegt, beweisen verschiedene Dokumente, die das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) auf seiner Webseite veröffentlicht hat.
Neben dem nicht selbstverständlichen Umstand, dass überhaupt bereits geprüft wird, geben diese Dokumente auch einen wertvollen Einblick in die datenschutzrechtliche Prüfpraxis des BayLDA. So ist ersichtlich, dass sowohl anlassunabhängig als auch bei solchen Unternehmen geprüft wird, bei denen bereits Verstöße festgestellt worden sind. Ferner wird vom BayLDA explizit darauf hingewiesen, dass sich die Prüfung nicht in der Zusendung und Beantwortung von Fragen erschöpft. Vielmehr werden die Unternehmen auch aufgefordert, Dokumente wie Informationsmuster nach Art. 13 DSGVO oder IT-Sicherheitskonzepte zur Glaubhaftmachung zu übersenden. Auch Vor-Ort-Prüfungen bleiben vorbehalten.

Wie sich aus den Dokumenten ergibt, wurden bisweilen Unternehmen unterschiedlichster Größe und mit Blick auf unterschiedliche Bereiche geprüft. So sind bisherige Adressaten sowohl drei Großkonzerne als auch diverse kleinere (ab 100 Mitarbeitern) und mittelständische Unternehmen (ab 500 Mitarbeitern) unterschiedlichster Branchen. Inhaltlich betreffen die Prüfungen verschiedene Bereiche des Datenschutzrechts in sehr unterschiedlichen Konkretisierungsgraden. So reichen die Prüfthemen von sehr konkreten Prüfblöcken wie das „Löschen von Daten bei ERP-Systemen (SAP)“ oder das „Patch Management eCommerce-Systeme/Online-Shops (Magento)“ bis hin zu scheinbar eher generischen Prüfmustern wie die „Umsetzung der DS-GVO bei kleinen und mittelständischen Unternehmen (KMUs)“. Der im zuletzt genannten Punkt veröffentlichte Fragebogen des BayLDA betrifft etwa Themen zur Bestellung und zum Aufgabenbereich des Datenschutzbeauftragten im jeweiligen Unternehmen, bestehende Niederlassungen und deren Einbindung in das Datenschutzkonzept, die Existenz eines Verarbeitungsverzeichnisses, das Bestehen und den Umsetzungsstand des IT-Sicherheitskonzepts, Prozesse zum Umgang mit Informations- und Betroffenenrechten sowie Fragen im Zusammenhang mit Datenschutzverletzungen.

Das BayLDA unterwirft dabei nicht jedes Unternehmen dem gleichen Prüfungsschema und beweist in diesem Zusammenhang eine nicht zu leugnende Praxisnähe. So ist sich das BayLDA offensichtlich insbesondere den Problemen größerer Unternehmen bewusst, ein datenschutzkonformes und konsistentes Löschkonzept zu implementieren und prüft nur solche Unternehmen, bei denen sie aufgrund der Unternehmensstruktur entsprechende Probleme vermutet. Ebenso wurden auch 15 größere Unternehmen nach den Informationspflichten gem. Art. 13 DSGVO im Zusammenhang mit dem Bewerbungsprozess befragt, deren Umsetzung erfahrungsgemäß häufig vernachlässigt wird.

Folgen für die Praxis:
Natürlich können aus den Veröffentlichungen keine vorbehaltlosen Schlüsse auf die diesbezügliche Praxis der Aufsichtsbehörden der anderen Bundesländer gezogen werden. Gleichwohl dienen die Informationen nicht nur in Bayern niedergelassenen Unternehmen als wertvolle Prüf- und Ansatzpunkte des eigenen datenschutzrechtlichen Umsetzungsstatus und sollten nicht ignoriert werden.

Die Veröffentlichungen des BayLDA zeigen, dass – wenn sie denn überhaupt je bestanden hat – eine etwaige Schonfrist für die Umsetzung der Datenschutzgrundverordnung abgelaufen zu sein scheint. Unternehmen, die die Datenschutzgrundverordnung bisher noch nicht oder nicht hinreichend umgesetzt haben, sollten diese Informationen weder ignorieren noch in Panik verfallen, sondern die wertvollen Hinweise des BayLDA als Unterstützung begreifen, um die eigene Umsetzung zu organisieren und den Umsetzungsstatus kritisch zu prüfen.

Dr. Hendrik Skistims, Frankfurt/Main

Nationale Datenschutzgesetze in der EU

Die meisten EU-Mitgliedstaaten haben ihre nationalen Datenschutzgesetze mittlerweile an die DSGVO angepasst. Als EU-Verordnung gilt die DSGVO zwar unmittelbar in jedem Mitgliedstaat. Ein nationales Umsetzungsgesetz ist gerade nicht mehr erforderlich. Die DSGVO enthält jedoch viele Regelungen, die durch die Mitgliedstaaten ausgefüllt werden können. Wichtige Beispiele sind der Beschäftigtendatenschutz, der Datentransfer in Drittstaaten und der betriebliche Datenschutzbeauftragte.
Zahlreiche Mitgliedstaaten haben ihre nationalen Datenschutzgesetze bereits so angepasst, dass sie zeitgleich mit der DSGVO am 25. Mai 2018 in Kraft treten konnten. Andere sind später nachgezogen.

Ohne entsprechendes auf die DSGVO abgestimmtes Datenschutzgesetz sind derzeit nur noch Bulgarien, die Tschechische Republik, Estland, Finnland, Griechenland, Portugal und Slowenien.

Obwohl die DSGVO als EU-Verordnung unmittelbar für die EU-Bürger gilt, wird der Datenschutz in den meisten EU-Mitgliedstaaten nicht nur durch die DSGVO geregelt. Für jegliche Datenschutzfragen muss nach wie vor in diesen Mitgliedstaaten auch die nationale Gesetzgebung herangezogen werden.

Dr. Oliver M. Bühr, Frankfurt/Main

3D-Druck und Produkthaftung: wer haftet?

Nach dem Produkthaftungsrecht in der Europäischen Union haften Hersteller von Produkten verschuldensunabhängig, wenn ein Produkt unsicher ist und dies zu einer Verletzung bestimmter Rechtsgüter führt (Leben, Körper, Gesundheit, privat genutzte Gegenstände). Andere Personen als Hersteller haften nur unter zusätzlichen Voraussetzungen.
Der Herstellerbegriff ist daher zentral im Produkthaftungsrecht. Werden Produkte im 3D-Druck hergestellt, ändern sich ggf. die Rollen, die es in der herkömmlichen Wertschöpfungskette (Zulieferer-Hersteller-Händler-Nutzer) gibt. Groß- und Einzelhändler kommen ggf. nicht vor, dafür kommen weitere Akteure dazu, wie der Ersteller der CAD-Datei, die die individuellen Befehle zur Steuerung des 3D-Druckers enthält und derjenige, der das Endprodukt ausdruckt (ein privater oder gewerblicher Nutzer oder ein zusätzlich eingeschalteter Dienstleister).

Das Produkthaftungsrecht – das gilt für Deutschland, aber auch alle anderen EU-Staaten – geht dagegen von der herkömmlichen Wertschöpfungskette aus und enthält Regelungen, die unmodifiziert diesen veränderten Rollen nicht gerecht werden. U.a. aus Gründen der richtigen Anreizsetzung (derjenige, der ein Risiko verhindern oder minimieren kann, sollte Anreize erhalten, dies im Rahmen des ökonomisch Vernünftigen zu tun), aber auch aus Gerechtigkeitserwägungen heraus, ist daher eine einerseits weite Auslegung des Herstellerbegriffs angezeigt. Andererseits scheint eine Einschränkung der Haftung der so einbezogenen Personen auf von ihnen beherrschte Herstellungsbereiche sachgerecht. Das führt zu folgenden Thesen:

1. Der Ersteller einer mit einem 3D-Scanner eingescannten Vorlage, als deren Abbild dann später das Endprodukt ausgedruckt wird, ist nicht Hersteller dieses Endprodukts.
2. Der Ersteller der CAD-Datei ist Hersteller des später ausgedruckten Endprodukts, was sich insbesondere daraus rechtfertigt, dass die CAD-Datei die den Druckvorgang steuernden Befehle enthält, die der Drucker „sklavisch“ abarbeitet. Seine Haftung beschränkt sich aber auf Fehler der CAD-Datei, die dann später auf das Endprodukt durchschlagen.
3. Auch derjenige, der das Produkt ausdruckt, ist Hersteller. Er haftet sowohl für Fehler, die aus einer fehlerhaften CAD-Datei folgen als auch für solche, die aufgrund von Fehlern beim Ausdruckvorgang selbst auftreten.
4. Setzt derjenige, der das Produkt ausdrucken will, dazu einen externen Dienstleister ein, bleibt er Hersteller, sofern er dem Dienstleister die Datei liefert und haftet für die Fehler des Endprodukts, unabhängig davon, ob diese schon in der CAD-Datei angelegt waren oder nicht.
5. Aber auch der den Drucker bedienende Dienstleister ist Hersteller; er haftet aber nicht für Fehler der ihm vorgegebenen CAD-Datei, die auf das Endprodukt durchschlagen.

Näheres zum Ganzen – auch unter dogmatischer Herleitung dieser Thesen – kann unserem Aufsatz: Korte/Istrefi, 3D-Druck und Produkthaftung, Der Betrieb 2018, Seite 2482-2486, entnommen werden.

Oliver Korte, Hamburg

Kundenzufriedenheitsumfragen per E-Mail sind Spam

Am 10. Juli 2018 erließ der Bundesgerichtshof eine weitere Entscheidung zum Thema Spamming, die sich auf die moderne Interaktion mit Kunden auswirkt. Gegenstand der Entscheidung war das Einholen von Kundenzufriedenheitsumfragen per E-Mail nach dem Kauf.

Nach Ansicht des Gerichts ist dies ohne ausdrückliche Zustimmung des Kunden offenkundig unerwünschte Werbung.

Kläger und Beklagte haben einen Kaufvertrag abgeschlossen. Der Kläger hat eine Rechnung per E-Mail mit folgendem Inhalt erhalten:

„Sehr geehrte Damen und Herren,

anbei erhalten Sie Ihre Rechnung im PDF-Format. Vielen Dank, dass Sie den Artikel bei uns gekauft haben. Wir sind ein junges Unternehmen und deshalb auf gute Bewertungen angewiesen. Deshalb bitten wir Sie darum, wenn Sie mit unserem Service zufrieden waren, uns für Ihren Einkauf eine 5-Sterne Beurteilung zu geben.

Sollte es an dem gelieferten Artikel oder unserem Service etwas auszusetzen geben, würden wir Sie herzlich darum bitten, uns zu kontaktieren. Dann können wir uns des Problems annehmen.

Zur Bewertung: über folgenden Link einfach einloggen und eine positive 5-Sterne Beurteilung abgeben (…)“

Während die ersten beiden Gerichte, die über den Fall zu entscheiden hatten, diese E-Mail als transaktionsbezogene Kommunikation und damit nicht als unrechtmäßige Zusendung unerlaubter Werbung betrachteten, hat der Bundesgerichtshof diese Auffassung zurückgewiesen.

Zunächst hat das Gericht (in Übereinstimmung mit der von den Vorinstanzen geäußerten Ansicht) festgestellt, dass Kundenzufriedenheitsbefragungen – da sie jedenfalls der Kundenbindung und damit der Förderung künftiger Geschäfte dienen – als Werbung zu betrachten sind.

Im konkreten Fall war die Gesamteinordnung der E-Mail durch das Gericht als Werbekommunikation die Folge der Verknüpfung der Rechnung mit der Umfrage zur Kundenzufriedenheit. Der Bundesgerichtshof stellte klar, dass der Versand einer Rechnung allein keine Werbung darstellt, aber – da die E-Mail-Adresse des Klägers von der Beklagten unter zwei Aspekten, nämlich für den Versand der Rechnung und zu Werbezwecken, verwendet worden ist – der Werbecharakter der E-Mail nicht durch die Verknüpfung der E-Mail mit transaktionsbezogener Kommunikation (Rechnung) aufgehoben werden konnte.

Das Gericht stellte fest, dass der Versand dieser E-Mail eine Verletzung der Persönlichkeitsrechte des Klägers darstellt.

Erläuternd wies das Gericht darauf hin, dass Werbung für ähnliche Produkte oder Dienstleistungen ohne die ausdrückliche Zustimmung des Empfängers zulässig sein kann. Diese Ausnahme erfordert jedoch einen klaren und eindeutigen Hinweis bei der Erhebung der E-Mail-Adresse des Kunden, dass der Kunde der Nutzung seiner Adresse jederzeit widersprechen kann, ohne dass hierfür weitere Kosten als die Übermittlungskosten anfallen.

Da eine solche Mitteilung der Beklagten fehlte, kam das Gericht zu dem Schluss, dass – da die Kundenzufriedenheitsumfrage im Allgemeinen als Werbung anzusehen ist – vorgenannte Ausnahme nicht geeignet sei, die Verletzung der Rechte des Empfängers (hier: Klägers) in vorliegendem Fall zu rechtfertigen.

Maximilian Wegge, München