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 03/2018

Der IT-Ticker 03/2018 informiert Sie über folgende Themen:

- Warnung vor der „Datenschutzauskunft-Zentrale“
- Einstweilige Verfügung wegen DS-GVO-Verstößen
- Blockchain & IP
- Datenschutzaufsichtsbehörde kündigt anlasslose Kontrollen an
- Erste konkrete Maßnahmenempfehlungen für die Umsetzung des Standard-Datenschutzmodells veröffentlicht
- Eine Geschichte von Dead Island, offenem WLAN-Zugang und Haftung
- Gilt die DS-GVO auch für Fotos und Filme?

Warnung vor aktuellen Faxmeldungen der „Datenschutzauskunft-Zentrale“

Aufsichtsbehörden warnen vor unberechtigten Aufforderungen zur Einhaltung des Datenschutzes. Seit Anfang Oktober werden Unternehmen, aber auch Selbständige und Vereine von einer sogenannten „Datenschutzauskunft-Zentrale“ per Fax kontaktiert. Übersendet wird eine „Eilige Fax-Mitteilung“, die den Eindruck erweckt, von einer Datenschutz-Aufsichtsbehörde zu stammen. Die Angeschriebenen sollen einer „Pflicht zur Umsetzung des Datenschutzes“ nachkommen und als „Basisdatenschutz-Beitrag“ jährlich 498,- Euro (oder sogar 592,- Euro) zahlen. Alleine die Zahlungspflicht sollte den Empfängern des Schreibens als Warnung dienen. Weder handelt es sich bei der „Datenschutzauskunft-Zentrale“ um eine Datenschutzaufsichts-Behörde im Sinne der Datenschutz-Grundverordnung (DS-GVO), noch können die Empfänger durch Rücksendung des Formulars und Entrichten des Beitrags datenschutzrechtlichen Pflichten der DS-GVO oder des BDSG nachkommen.

Mehrere Datenschutz-Aufsichtsbehörden haben sofort mit Stellungnahmen auf die E-Mail-Flut der „Datenschutzauskunft-Zentrale“ reagiert. Die Aufsicht warnt dringend davor, auf die Fax-Anschreiben zu antworten. Thüringens Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) empfiehlt zudem, im Falle, dass das Schreiben unterschrieben zurückgeschickt worden ist, die abgegebenen Erklärungen umgehend zu widerrufen. Der Präsident des bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) weist ausdrücklich darauf hin, dass die Aufforderungen des Versenders in keiner Weise mit der seit dem 25. Mai 2018 geltenden DS-GVO in Verbindung stehen. Es sei erschreckend, mit welchen Methoden versucht wird, teilweise bestehende Unsicherheiten bei der Umsetzung der DS-GVO auszunutzen, so der Präsident des BayLDA.

Auch die Presse hat den Fall aufgegriffen und warnt vor der „Datenschutzauskunft-Zentrale“ (heise.de, SPIEGEL Online).

Praxistipp:
Wir empfehlen, auf die Aufforderung der „Datenschutzauskunft-Zentrale“ nicht zu reagieren und sich bei Empfang eines solchen Schreibens umgehend an den betrieblichen bzw. behördlichen Datenschutzbeauftragten zu wenden.

Generell sollte bei Aufforderungen, die nur per Fax kommen und offiziell aussehen, der Text sehr genau gelesen werden.

Ivan Brankov, Frankfurt/Main
Nikolaus Bertermann, Berlin

Einstweilige Verfügung wegen DS-GVO-Verstößen

Mit Beschluss vom 13. September 2018 (11 O 1741/18 UWG) hat das Landgericht Würzburg eine einstweilige Verfügung gegen eine Anwältin erlassen, die auf Ihrer Webseite keine vollständigen Datenschutzhinweise bereitgestellt hat und auf deren unverschlüsselter Webseite ein Kontaktformular angeboten wurde.
Das Gericht sah sowohl in den fehlenden Datenschutzhinweisen als auch in der fehlenden Verschlüsselung der Webseite jeweils einen Verstoß gegen die DSGVO. Hinsichtlich der fehlenden Datenschutzhinweise ist dies nachvollziehbar, warum das Gericht aber in der fehlenden Verschlüsselung einen Datenschutzverstoß erkennt, erläutert es nicht. Dies ist bereits technisch fragwürdig, da die Übermittlung von Formulardaten häufig per E-Mail erfolgt, so dass die Verschlüsselung der Webseite technisch gar keinen Einfluss auf die Übermittlung der Formulardaten hätte.

Das Gericht entschied weiter, dass damit jeweils auch ein Verstoß gegen Marktverhaltensregeln vorliege und entsprechend Unterlassungsansprüche nach dem Gesetz gegen unlauteren Wettbewerb (UWG) bestehen. Dafür verweist das Gericht auf zwei Entscheidungen des OLG Hamburg und des OLG Köln, die jeweils noch vor Inkrafttreten der DSGVO zu datenschutzrechtlichen Regelungen des TMG ergangen sind. Dass jedenfalls die überwiegende Auffassung der Fachliteratur die Regelungen der DS-GVO als abschließend erachtet und deshalb eine Anwendung des UWG auf Datenschutzverstöße ablehnt, erwähnt das Gericht nicht.

Da die Entscheidung im einstweiligen Rechtsschutz und ohne Anhörung der Antragsgegnerin ergangen ist, ist sie mit Vorsicht zu bewerten. Es bleibt abzuwarten, ob die Entscheidung Bestand hat.

Praxistipp:
Vollständige Datenschutzinformationen auf der Webseite sind nach der DSGVO unstreitig erforderlich und sollten von allen Webseitenbetreibern umgesetzt werden – unabhängig von der Frage, ob eine unvollständige Erklärung auch einen Wettbewerbsverstoß darstellt. Wenn Kontaktformulare auf der Webseite angeboten werden und die Übermittlung der Daten von der Webseite an den Betreiber nicht verschlüsselt erfolgt, sollte jedenfalls auf die unverschlüsselte Übermittlung der Daten hingewiesen werden.

Update:
Das Landgericht Bochum hat in einem Beschluss vom 7. August 2018 einen Unterlassungsanspruch zwischen Wettbewerbern wegen eines Verstoßes gegen die DSGVO abgelehnt. In seiner Begründung verwies es darauf, dass dem Verfügungskläger ein Anspruch Unterlassung deshalb nicht zustehe, weil die Datenschutzgrundverordnung Regelungen enthalte, welche abschließend sind und deshalb Ansprüche von Mitbewerbern ausschließen. Zur Begründung nahm das Gericht ausdrücklich Bezug auf eine in der Rechtsliteratur weit verbreitete (und oben angeführte) Meinung.

Florian Hensel, München
Nikolaus Bertermann, Berlin

Blockchain & IP

Die Blockchain ist derzeit in aller Munde. Einer ihrer großen Vorteile ist es, dass sie als besonders sicher gilt. Die Blockchain ist durch Kryptowährungen wie Bitcoin bekannt geworden. Sie wird aber nicht mehr nur für Kryptowährungen genutzt, sondern in den verschiedensten Branchen. Noch steht die Entwicklung am Anfang und es existieren technische und rechtliche Hürden. Dennoch beschäftigen sich derzeit zahlreiche Unternehmen und Arbeitskreise mit der Blockchain, auch im Bereich des gewerblichen Rechtsschutzes. Auch das Amt der Europäischen Union für geistiges Eigentum (EUIPO) untersucht aktiv die Möglichkeiten von Blockchain (siehe https://euipo.europa.eu/ohimportal/de/news/-/action/view/4121074). Einige der Überlegungen, die im Bereich des gewerblichen Rechtsschutzes derzeit angestellt werden, möchten wir Ihnen mit diesem Beitrag zeigen.
Warum kann die Blockchain im gewerblichen Rechtsschutz von Vorteil sein?

Blockchains sind Datenbanken, in denen bestimmte Ereignisse bzw. Transaktionen in chronologischer Reihenfolge hinterlegt werden. Im Unterschied zu herkömmlichen Datenbanken handelt es sich um

dezentrale Datenbanken, die sich auf den Rechnern aller Teilnehmer der Blockchain befinden. Die Datenbanken sind nicht wie herkömmlich an einer zentralen Stelle hinterlegt.

Informationen werden in der Blockchain direkt vom Sender zum Empfänger geleitet, ohne dass der Einsatz von Dritten erforderlich ist. Jede Transaktion in der Datenbank wird durch eine komplexe technische Einstellung bewertet und verifiziert. Erst nach der Verifizierung wird die Transaktion zu der Kette hinzugefügt und in der Datenbank hinterlegt. Alle Teilnehmer erhalten eine Kopie der jeweiligen Transaktion. Die hinterlegten Transaktionen und Ereignisse sind daher unveränderbar. Informationen gehen nicht verloren.

Da das Netzwerk der Blockchain dezentral ausgestaltet ist, eine komplexe Verschlüsselung eingesetzt wird und weil die Transaktionen in einer zeitlichen Abfolge transparent verkettet werden, gelten schädigende Hacker-Eingriffe und das Verfälschen von Daten in der Blockchain als beinahe unmöglich. Die Blockchain gilt daher als besonders sicher und vertrauenserweckend. Da keine zentrale Prüfstelle existiert, können Transaktionen zeitlich sehr schnell erledigt werden. Die Technik gilt daher auch als sehr effizient. Vor diesem Hintergrund kann die Technik in folgenden Bereichen des gewerblichen Rechtsschutzes interessant sein:

Verwaltung und Nachweis von Rechten

Denkbar wäre eine Datenbank auf Blockchain-Basis mit Angaben rund um ein Schutzrecht. Die Datenbank könnte Angaben dazu enthalten, wann ein Schutzrecht angemeldet, registriert, lizenziert oder gewerblich verwendet wurde. Über Schnittstellen in den Handel, wo das Schutzrecht wie beispielsweise die Marke oder das Design genutzt wird, könnten die gewünschten Informationen bezüglich der Verwendung unmittelbar in die Datenbank gemeldet werden. In Amts- oder Gerichtsverfahren würden Nutzungsnachweise unkompliziert geführt und Beweisprobleme vermieden werden. Diese Technik kann eine wesentliche Erleichterung beim Nachweis der Erstverwendung, der ernsthaften Benutzung und die Anerkennung bekannter Marken bringen.

Durch eine dezentrale Erfassung der Informationen würde das Management der einzelnen Schutzrechte durch die Sicherheit, die die Blockchain bietet, noch zuverlässiger und effektiver. Übernahmen von Schutzrechteportfolien könnten durch die sichere und vertrauenswürdige Technik unkomplizierter stattfinden.

Durchsetzung von IP-Rechten

Im Bereich des gewerblichen Rechtsschutzes können sog. Smart Contracts auf Blockchain-Basis interessant sein. Smart Contracts sind Computerprogramme auf Blockchain-Basis, in denen Vertragsbedingungen in Form von Wenn-Dann-Regelungen hinterlegt sind. Diese Vertragsbedingungen werden selbständig ausgeführt und überwacht (zur Funktionsweise siehe: https://www.skwschwarz.de/aktuelles/artikel/artikel-detail/news/smart-contracts-intelligente-vertraege-der-zukunft/4/detail/News/).

Smart Contracts können den Schutz und die Durchsetzung von IP-Rechten automatisieren. Smart Contracts könnten z.B. eingesetzt werden, um Lizenzen zu vergeben oder allgemein um Verträge zu erstellen und durchzusetzen. Hierzu würde in dem Smart Contract die Regel hinterlegt, dass ein Recht eingeräumt wird, sobald die Gegenleistung (z.B. Zahlung) erbracht wurde. So könnte die Übertragung von Rechten in Echtzeit an die Zahlung geknüpft werden. Separate Durchführungsakte wie das Registrieren des Geldeingangs sind nicht mehr erforderlich. Im Bereich der Musikindustrie existieren bereits erste Plattformen auf Blockchain-Basis, die die Urheberrechte der Künstler an den Titeln automatisch verwalten. Durch den Smart Contract erhält der Künstler automatisch und in Echtzeit die ihm zustehende Abgabe, wenn ein Kunde einen Musiktitel kauft (siehe https://peertracks.com/).

Verfolgung von Rechtsverstößen in der Lieferkette

Großes Potenzial der Blockchain-Technologie wird auch in der Verfolgung von Rechtsverstößen in der Lieferkette gesehen, wie z.B. in der Verfolgung von Produktpiraterie und in der Verfolgung von Verstößen in Vertriebssystemen. Durch eine Registrierung mit der Blockchain-Technologie könnten Produkte nachverfolgt werden. Die Produkte würden durch die ihnen hinterlegte Technik (z.B. Codes oder Siegel) Informationen in die Blockchain melden, wo und wann sie sich befinden und ggfs. wer welches Produkt besitzt. So könnten die Teilnehmer der Blockchain die Produkte stets in der

Vertriebskette verfolgen. Zusätzlich könnten weitere Informationen, z.B. zur Produktion und Qualität, zu dem Produkt hinterlegt werden. Das bringt die Möglichkeit Produkte zu verifizieren, denn es ist z.B. ersichtlich, dass das Markenprodukt keine Fälschung darstellt. Der Verbraucher hätte größere Sicherheit, dass er kein gefälschtes Produkt erwirbt. Gestohlene Produkte könnten wieder aufgefunden werden. Auch der Zoll könnte sich diese Informationen zu Nutze machen. Eine weitere Chance des Einsatzes der Blockchain liegt darin, dass durch die Nachverfolgbarkeit der Produkte Lecks in Vertriebssystemen ohne größeren Aufwand aufgedeckt werden könnten.

Zusammenfassung und Fazit

Zusammenfassend kann die Blockchain-Technologie im Bereich des gewerblichen Rechtsschutzes aufgrund der Sicherheit und Transparenz kosteneffektive Möglichkeiten bieten, den Nachweis von Schutzechten zu führen, IP-Rechte durchzusetzen oder Rechtsverstöße in der Lieferkette zu verfolgen. Da das Thema Blockchain nicht nur in Unternehmen und Verbänden, sondern auch in der Regierung und den Markenämtern an Bedeutung gewinnt, ist es wünschenswert, dass der Gesetzgeber rechtliche Hürden bei der Anwendung der Blockchain-Technologie z.B. durch Gesetzesänderungen nehmen wird, damit die Technik in Zukunft breitflächig eingesetzt werden kann.

Yvonne Schäfer, Frankfurt/Main

Datenschutzaufsichtsbehörde kündigt anlasslose Kontrollen an

Die Datenschutzgrundverordnung (DSGVO) gibt den Aufsichtsbehörden u.a. die Aufgabe auf, die Anwendung der Verordnung zu überwachen und durchzusetzen. Die Aufsichtsbehörde kann sich dafür auf die Eingaben und Beschwerden von Betroffenen verlassen. Sie hat aber auch die Möglichkeit aus eigenem Entschluss tätig zu werden und sogenannte anlasslose Kontrollen bei den Verantwortlichen für die Datenverarbeitung durchzuführen. Solche Kontrollen werden von Unternehmen besonders gefürchtet, da sie die Unternehmen zwingen, innerhalb eines von der Behörde vorgegebenen kurzen Zeitraums unter Umständen eine Vielzahl von Informationen aufzubereiten und zu verifizieren, ohne in diesem Moment auf diese Anfrage vorbereitet zu sein. Das bayerische Landesamt für Datenschutzaufsicht als Aufsichtsbehörde hat nun seine Sichtweise auf diese Kontrollen öffentlich gemacht, um den Unternehmen in Bayern die Möglichkeit zu verschaffen, sich auf Kontrollen besser vorbereiten zu können. Die Aufsichtsbehörde legt dabei hohen Wert auf die Transparenz ihrer Aktivitäten. Sie hat daher angekündigt alle verwendeten Prüffragebögen auf ihrer Homepage (www.lda.bayern.de) zu veröffentlichen und dort auch die Ergebnisse der Kontrollen zu dokumentieren. Die Kontrollen werden stichprobenartig erfolgen. Sollten dabei Verstöße festgestellt werden, ist mit Anordnungen (z.B. zur Untersagung der Datenverarbeitung) oder Sanktionen wie Bußgeldern zu rechnen.

Ein besonderes Zeichen der Bereitschaft zur Transparenz seitens der Aufsichtsbehörde ist die Veröffentlichung des für die kommenden Wochen und Monate geplanten Prüfungsplans für Kontrollen in Bayern. Demnach sind zunächst folgende Kontrollen geplant:

- September 2018: Prüfung Rechenschaftspflicht von (erstmal drei) Großunternehmen
- September 2018: Cybersicherheit: Verschlüsselungstrojaner bei Arztpraxen (erstmal 8 Praxen)
- Oktober 2018: Erfüllung der Informationspflichten in Bewerbungsverfahren (bei erstmal 25 Unternehmen)
- Oktober 2018: Cybersicherheit: Patch-Management bei (erstmal 15) Online-Diensten
- November 2018: Cybersicherheit: Erkennung von Datenschutzverletzungen bei internationalen Sub-Dienstleistern (erstmal 5 Großunternehmen).

Es bedarf sicherlich keines besonderen prophetischen Talents, um vorherzusagen dass andere Aufsichtsbehörden in Deutschland und Europa diesem Beispiel der bayerischen Aufsichtsbehörde folgen werden und eigene Kontrollen durchführen werden. Die niedersächsische Aufsichtsbehörde führt bereits seit Juni 2018 umfassende Querschnittskontrollen (zunächst bei 20 großen und 30 mittelgroßen Unternehmen) durch(https://www.lfd.niedersachsen.de/startseite/allgemein/presseinformationen/querschnittspruefung_fragen_zur_dsgvo_an_50_unternehmen/fragen-zur-ds-gvo-an-50-unternehmen-166110.html). Es ist daher die Aufgabe der Unternehmen das Angebot der Aufsichtsbehörde zur Transparenz ernst zu nehmen und sich auf diese Kontrollen bestmöglich vorzubereiten.

Praxistipp:
Da die Aufsichtsbehörde angekündigt hat, alle Prüfbögen auf ihrer Homepage öffentlich zu machen, lohnt sich ein regelmäßiger prüfender Blick auf diese Homepage zum einen als Vorbereitung auf mögliche Kontrollen aber auch als hilfreiche Checkliste zur Prüfung der eigenen Datenschutz Compliance.

Dr. Matthias Orthwein, München

Erste konkrete Maßnahmenempfehlungen für die Umsetzung des Standard-Datenschutzmodells veröffentlicht

Anwender des Standard-Datenschutzmodells können die ersten Bausteine eines umfassenden Maßnahmenkatalogs zu Themen wie Aufbewahrung, Löschung, Protokollierung und andere in der Praxis erproben.
Als Standard-Datenschutzmodell (SDM) bezeichnen die Datenschutzaufsichtsbehörden der Länder und des Bundes ein Modell (DSK), mit dem die Übereinstimmung der gesetzlichen Anforderungen im Umgang mit personenbezogenen Daten und der entsprechenden Umsetzung dieser Vorgaben systematisch überprüfbar gemacht wird. Die Methode orientiert sich dabei an zentralen Gewährleistungszielen, wie etwa Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz etc., die über technische und organisatorische Funktionen und Schutzmaßnahmen umgesetzt werden. Das SDM richtet sich insbesondere an die Stellen, die für die Verarbeitung personenbezogener Daten verantwortlich sind. Diese können mit dem SDM die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen.

Ein wichtiger Bestandteil des Standard-Datenschutzmodells ist ein Maßnahmenkatalog mit konkreten Vorgaben zur Gewährleistung dieser Ziele. Dieser Katalog (Kapitel 7 des SDM) besteht aus unterschiedlichen Bausteinen zu datenschutzrechtlich relevanten Themenkomplexen. Nun wurden die ersten Bausteine von der zuständigen Arbeitsgruppe veröffentlicht. An die Erarbeitung dieser haben der Hessische Beauftragte für Datenschutz und Informationsfreiheit, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, der Sächsische Datenschutzbeauftragte, das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland mitgewirkt.

Folgende Bausteine wurden veröffentlicht:

- Datenschutz-Management
- Planung / Spezifikation
- Dokumentation
- Protokollierung
- Trennung
- Löschen und Vernichten
- Aufbewahrung

Die Bausteine enthalten konkrete technische und organisatorische Referenzmaßnahmen zur Gewährleistung der je nach Themenkomplex relevanten datenschutzrechtlichen Ziele wie Vertraulichkeit, Integrität Datenminimierung usw. Die einzeln aufgezeigten Handlungsmöglichkeiten werden dabei einzelnen Kategorien zugeordnet, je nachdem, ob die jeweilige Maßnahme auf Daten-, System- oder Prozessebene getroffen werden muss. Über eine ausführliche Beschreibung der einzelnen zu treffenden Maßnahmen hinaus enthalten die Bausteine auch eine Zusammenfassung dieser in Form einer Liste sowie Referenzen auf weitere Unterlagen wie z.B. Stellungnahmen des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder der DSK, DIN- und ISO-Normen.

Es ist zu berücksichtigen, dass die Autoren der neu erarbeiteten Bausteine ausdrücklich darauf hinweisen, dass diese Bausteine noch nicht in der DSK abgestimmt worden sind. Ziel dieser ersten Veröffentlichung ist, den Anwendern schon konkrete Maßnahmenempfehlungen zu geben, die sie erproben können. Die beteiligten Aufsichtsbehörden empfehlen den Anwendern, ihre Erfahrungen bei der Implementierung der Bausteine den Autoren mitzuteilen und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Praxistipp für Unternehmen:
Auch wenn die Bausteine nicht mit der DSK abgestimmt worden sind, muss beachtet werden, dass

diese gleichwohl von vier Datenschutz-Aufsichtsbehörden erarbeitet wurden und damit durchaus das vorläufige Meinungsbild der Aufsicht zu den jeweiligen Themenkomplexen widerspiegeln. Es empfiehlt sich aus diesem Grund, den Maßnahmenkatalog des SDM anzuwenden und die im Unternehmen getroffenen technisch-organisatorischen Maßnahmen an den im SDM dargestellten Empfehlungen zu messen und ggf. anzupassen. Unternehmen sollten darüber hinaus die Veröffentlichung der weiteren Bausteine des Maßnahmenkatalogs beobachten.

Ivan Brankov, Frankfurt/Main

Eine Geschichte von Dead Island, offenem WLAN-Zugang und Haftung

Für sein ziemlich kreatives Rechtskonzept rund um die Mitwirkungshaftung, wörtlich als „Störerhaftung" bezeichnet, hat Deutschland mittlerweile eine gewisse Berühmtheit erlangt. Der Bundesgerichtshof scheint in seiner „Dead Island"-Entscheidung den Unterlassungsansprüchen gegen Betreiber von offenen WLANs in Bezug auf Schutzrechtsverletzungen, die Dritte über deren Zugangspunkte begangen hatten, ein Ende bereitet zu haben.
Die Entscheidung schien notwendig, um die Interessen von Urheberrechtsinhabern und Inhabern anderer geistiger Eigentumsrechte, die europäischen Rahmenbedingungen für unsere moderne Informationsgesellschaft und den Schutz des geistigen Eigentums und nicht zuletzt von Einzelpersonen in Einklang zu bringen. Was in Anbetracht des Art. 12 der E-Commerce-Richtlinie 2000/31/EG und ihrer Grundsätze in Bezug auf Zugangsanbieter als „reine Durchleitung" als ein geradezu offensichtliches Ergebnis erscheinen mag, könnte durchaus dazu dienen, ein 15 Jahre altes Kapitel einer Rechtsdurchsetzungsstrategie zu einem Ende zu bringen.

Hintergrund ist, dass ein Spielehersteller einen IT-Spezialisten, der mehrere offene Internet-Zugangspunkte über WLAN sowie zwei Tor Exit-Nodes betrieben hatte, im Zusammenhang mit Urheberrechtsverletzungen im Spiel „Dead Island", die über die Netzwerkzugriffspunkte begangen wurden, verklagte. Da der eigentliche Verletzer oft nicht identifiziert und in Anspruch genommen werden kann, ist der Betreiber des Netzwerkzugriffspunktes in der Regel die beste Wahl für die Rechteinhaber. Der Bundesgerichtshof hatte bisher die Haftungsfilter der E-Commerce-Richtlinie so ausgelegt, dass sie keine Unterlassungsansprüche abdecken, und einen sehr differenzierten Haftungsrahmen rund um „kausale Beiträge" und „angemessene Pflichten" geschaffen – was für die Anbieter von Zugangspunkten ein erhebliches wirtschaftliches Risiko darstellte. Um die Verbreitung von offenem WLAN zu fördern und die Gefährdung der Betreiber zu verringern, hatte der deutsche Gesetzgeber spezielle Vorschriften erlassen, die die Zugangsanbieter ausdrücklich von der Haftung im Zusammenhang mit Verstößen der Nutzer, einschließlich Unterlassung, Wiedergutmachung usw., freistellten. Es war jedoch unklar, ob das Gesetz mit anderen europäischen Vorschriften, nämlich Art. 11 Satz 3 der Durchsetzungsrichtlinie, in Einklang steht, die die Mitgliedstaaten verpflichtet, Rechtsinhaber in die Lage zu versetzen, in diesem Zusammenhang Anordnungen gegen Mittler zu erreichen.

Das Gericht hat nun in diesem Zusammenhang lediglich die Störerhaftung auf Unterlassen aufgehoben, das neue Gesetz bestätigt und die Rechteinhaber auf eine weitere neue Möglichkeit im Gesetz hingewiesen: die Erlangung einer Anordnung auf „Sperrung des Zugangs zu Informationen", um weitere Verstöße zu verhindern. Obwohl sich dies wieder an den WLAN-Betreiber richtet, wies das Gericht jedoch darauf hin, dass verschiedene Maßnahmen angemessen sein können, die von der Registrierung von Nutzern, der Verschlüsselung des Zugangs mit einem Passwort und – ausdrücklich als äußerstem Fall – bis zur vollständigen Sperrung des Zugangs reichen können. Dies erlaubt es Zugangsbetreibern wohl, bevor sie die Nutzer auf einem „Dead Island" zurücklassen, eine Reihe anderer Maßnahmen zu ergreifen, anstatt einer Zugangssperre, ohne für Kosten oder unmittelbare Unterlassung haftbar zu sein. Nun liegt es wieder am Gericht zweiter Instanz, die Rechtssache den Maßgaben des Bundesgerichtshofs zu entscheiden.

Florian Hensel, München

Gilt die DS-GVO auch für Fotos und Filme?

Spätestens seit dem 25. Mai 2018 stellt sich bei den verschiedensten digitalen Anwendungen/Vorgängen die Frage, ob die neuen Datenschutzregelungen beachtet werden müssen. Die neuen Datenschutzregelungen aus der Europäischen Datenschutzgrundverordnung (DSGVO) und dem neuen Bundesdatenschutzgesetz (BDSG) müssen immer dann beachtet werden, wenn personenbezogene Daten im nicht privaten Bereich verarbeitet werden.
Verarbeitung personenbezogener Daten

Auch Fotos (ebenso wie Filme) können personenbezogene Daten enthalten. Zum einen ist das Gesichtsbild ein personenbezogenes Datum, zum anderen werden häufig zu den einzelnen digitalen Fotos weitere Daten wie Ort und Zeit der Bildaufnahme oder andere GPS-Informationen als Metadaten gespeichert. Hochauflösende Aufnahmen in HD Qualität ermöglichen oft auch eine biometrische Erkennung der abgebildeten Personen. In diesem Fall handelt es sich sogar um besonders geschützte sensible personenbezogene Daten (Art. 9 DSGVO).

Rechtsgrundlage für die Datenverarbeitung

Wenn personenbezogene Daten verarbeitet werden, dann muss das rechtmäßig erfolgen, d.h. es muss eine Rechtsgrundlage nach Art. 6 DSGVO bestehen. In diesem Zusammenhang stellt sich allerdings die berechtigte Frage, welche Rolle das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (auch Kunsturhebergesetz, KUG) noch spielt. Wird das KUG durch die DSGVO gegenstandslos? Oder gelten für Fotografien die KUG-Regelungen als speziellere Regelungen?

Zu diesen Fragen hat die Datenschutzaufsichtsbehörde des Landes Brandenburg nun Stellung genommen (LDA Brandenburg: „Verarbeitung personenbezogener Daten bei Fotografien“, abrufbar unter: https://www.lda.brandenburg.de/media_fast/4055/DSGVOFotografienfinal.pdf). Die Aufsichtsbehörde stellt klar, dass das Kunsturhebergesetz nur Regelungen zur Verbreitung und öffentlichen Zurschaustellung von Fotos enthält. Für das eigentliche „Fotografieren“, d.h. die Herstellung des Lichtbildes finden sich keine Regelungen im KUG. Insoweit muss in jedem Fall auf Rechtsgrundlagen der DSGVO zurückgegriffen werden, wie die Einwilligung, die Vertragsdurchführung oder das berechtigte Interesse.

Rechtsgrundlage für das Fotografieren

Als Rechtsgrundlage kommt demnach eine datenschutzrechtliche Einwilligung in Betracht. Problematisch an dieser Rechtsgrundlage ist jedoch, dass der Einwilligende das Recht hat, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Das kann dazu führen, dass das Foto wieder gelöscht werden muss und nicht mehr verwendet werden darf. Darüber hinaus verlangt die DSGVO eine ausführliche Information des Betroffenen, damit seine Einwilligung überhaupt wirksam ist. Vor diesem Hintergrund empfiehlt es sich eine andere Rechtsgrundlage zu wählen, wenn eine solche verfügbar ist.

Das Anfertigen von Fotos kann auch erlaubt sein, weil der Fotografierte einen Vertrag mit dem Fotografen über die Fotoaufnahmen geschlossen hat. Weitere Personen dürfen aufgrund dieses Vertrages allerdings nicht fotografiert werden.

Neben der Vertragsdurchführung und der Einwilligung kommt außerdem die Verarbeitung (hier: das Fotografieren) aufgrund eines überwiegenden berechtigten Interesses in Betracht. Hierbei müssen die schutzwürdigen Interessen der Beteiligten gegeneinander abgewogen werden. Als Interessen des Fotografen kommen u.a. in Betracht, dass er seine berufliche Betätigung ausüben möchte, die u.a. der Berufs- oder Kunstfreiheit unterliegt, oder das Interesse des Veranstalters (als Interesse Dritter) eine Veranstaltung zu dokumentieren. Diesen Interessen sind die Interessen des Fotografierten gegenüberzustellen. Die Interessen des Fotografierten richten sich nach den vernünftigen Erwartungen des Fotografierten. So muss der Fotografierte bei öffentlichen oder großen Veranstaltungen damit rechnen, dass die Veranstaltung auf Fotos dokumentiert wird. Heimliche oder diskreditierende Aufnahmen werden hingegen dem berechtigten Interesse des Fotografen nicht überwiegen, so dass solche Fotografien ganz überwiegend nicht auf Grundlage des berechtigten Interesses erfolgen können. Als weitere Beispiele, in denen sich der Fotograf nicht auf seine berechtigten Interessen stützen kann, führt das LDA Brandenburg auch das Fotografieren von Kindern an und Fotos mit Personen, die Bezug nehmen auf die Religion, Gesundheit, das Sexualleben oder die sexuelle Orientierung des Fotografierten. Zuletzt genannte Situationen fallen ebenso wie die biometrischen Daten unter die besonderen Kategorien personenbezogener Daten, die nach Artikel 9 DSGVO besonders schützenswert sind.

Rechtsgrundlage für das Verwenden von Fotos

Für die Verwendung von Fotos, wie das Veröffentlichen, könnte hingegen das KUG vorrangig gelten. § 22 KUG bestimmt, dass Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. § 23 KUG regelt Situationen, in denen ausnahmsweise keine Einwilligung erforderlich ist, wie z.B. bei Aufnahmen von Versammlungen oder wenn die Person nur zufällig („als Beiwerk“ eines Ortes) auf das Bild geraten ist. Ob das KUG neben der DS-GVO anwendbar bleibt, ist derzeit unklar.

Die DSGVO sieht in Art. 85 Abs. 1 und 2 vor, dass die Mitgliedstaaten für journalistische, wissenschaftliche, künstlerische, und literarische Zwecke konkrete Abweichungen von der DSGVO vorsehen müssen bzw. können, damit Meinungsäußerungs- und Informationsfreiheit gewahrt bleiben. Ob Deutschland bisher solche Regelungen getroffen hat, ist unklar. Nach derzeitigen Informationen hat Deutschland zumindest keine Ausnahmegesetze an die Kommission gemeldet. Möglicherweise stellt das KUG eine Rechtsvorschrift nach Art. 85 Abs. 1 DSGVO dar, für die keine Meldung an die Kommission erforderlich ist. Insoweit besteht derzeit Rechtsunsicherheit. Das Bundesministerium des Innern, für Bau und Heimat hat hierzu eine Stellungnahme veröffentlicht (abrufbar unter: https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html#f10924666), die unabhängigen Datenschutzbehörden hingegen haben sich bisher nicht positioniert. Auch das LDA Brandenburg positioniert sich mit der oben genannten Stellungnahme hierzu nicht. Es sagt lediglich, dass für die Verwendung von Fotos die Einwilligung des Fotografierten oder eine andere Rechtsgrundlage erforderlich sei. Die Ausnahmevorschriften des § 23 KUG könnten zumindest im Rahmen einer Interessenabwägung bei einer Verarbeitung auf Grundlage berechtigter Interessen berücksichtigt werden, solange keine anderslautenden Regelungen getroffen würden.

Um Rechtsunsicherheiten zu vermeiden empfiehlt es sich, wenn möglich für das Veröffentlichen von Personenfotografien eine Einwilligung einzuholen.

Ausnahmevorschriften für die Presse

Ausnahmen bestünden immerhin für die Presse, denn hier gilt nach Auffassung des LDA Brandenburg weiterhin das sog. Medienprivileg. Für das Fotografieren und Verbreiten von Fotos zu journalistisch-redaktionellen Zwecken sei das Medienprivileg, das zum einen im Rundfunkstaatsvertrag (RStV) in § 9 c RStV und § 57 RStV, und zum anderen in verschiedenen landesrechtlichen Gesetzen geregelt ist, eine Vorschrift nach Art. 85 Abs. 1 DSGVO. Die Presse ist hierdurch von zahlreichen Vorschriften der DSGVO befreit. Dabei ist allerdings darauf zu achten, dass nur die journalistisch verfasste Presse (z.B. Zeitung oder Fotoreporter, u.U. auch Blogs) unter diese Befreiung fällt. Die Presseabteilung eines Unternehmens wird sich auf diese Befreiung wohl nicht berufen können.

Informationspflichten

Da personenbezogene Daten verarbeitet werden, müssen die Informationspflichten nach Art. 13, 14 DSGVO erfüllt werden. Die Datenschutzaufsicht Brandenburg empfiehlt, dass die Datenschutzhinweise in Einladungen oder auf Hinweisschildern bei einer Veranstaltung mitgeteilt werden. Bei Fotos mit einer Vielzahl von Personen kann im Einzelfall die Informationserteilung unverhältnismäßig sein, so dass nach Art. 14 Abs. 5 DSGVO ausnahmsweise nicht informiert werden müsste. Denkbar könnte das in einem nicht umgrenzten Raum in der Öffentlichkeit sein, wenn Personen nicht erreicht werden können, z.B. in der U-Bahn oder auf öffentlichen Plätzen. Insoweit ist jedoch stets der Einzelfall zu betrachten.

Löschpflichten

Personenbezogene Daten und damit auch Fotos, die Personen abbilden, sind zu löschen, sobald diese nicht mehr benötigt werden. So lange die Daten allerdings zur Durchsetzung von Rechtsansprüchen erforderlich sind, besteht keine Löschpflicht. Das Gesetz über Urheberrecht und verwandte Schutzrechte (auch Urheberrechtsgesetz, UrhG) bestimmt, wie lange Werke Schutz genießen. Hiernach genießen Fotos 70 Jahre nach dem Tod des Urhebers, also des Fotografen, Urheberrechte. So lange bestehen keine Löschpflichten. Durch das Medienprivileg oder andere Vorschriften können evtl weitere abweichende Löschpflichten bestehen, wenn beispielsweise ein historisches Interesse an der Aufbewahrung der Fotos bestünde.

Fazit

Wenn auf Fotos Personen identifiziert werden können, handelt es sich um personenbezogene Daten. Damit müssen die Datenschutzgesetze beachtet werden, wenn nicht ausschließlich im privaten Bereich fotografiert und veröffentlicht wird. Fest steht, dass für das Fotografieren die DSGVO gilt. Ob für das Veröffentlichen oder anderweitige Nutzen von Fotos, auf denen Personen abgebildet sind, vorrangig das KUG gilt, ist derzeit offen. Es bleibt auch abzuwarten, ob weitere Erleichterungen durch Gesetze beschlossen werden. Bisher bekanntgewordene Entwürfe zur Überarbeitung des KUG bieten jedenfalls noch keine hinreichenden Lösungen für die oben aufgeworfenen Fragen.

Solange die Aufsichtsbehörden und Gerichte sich nicht positionieren, empfiehlt sich derzeit wenn möglich die Einholung einer Einwilligung der Fotografierten zur Veröffentlichung von Fotos um Rechtsunsicherheiten auszuschließen. In jedem Fall sollte im zumutbaren Rahmen informiert werden.

Yvonne Schäfer, Frankfurt/Main