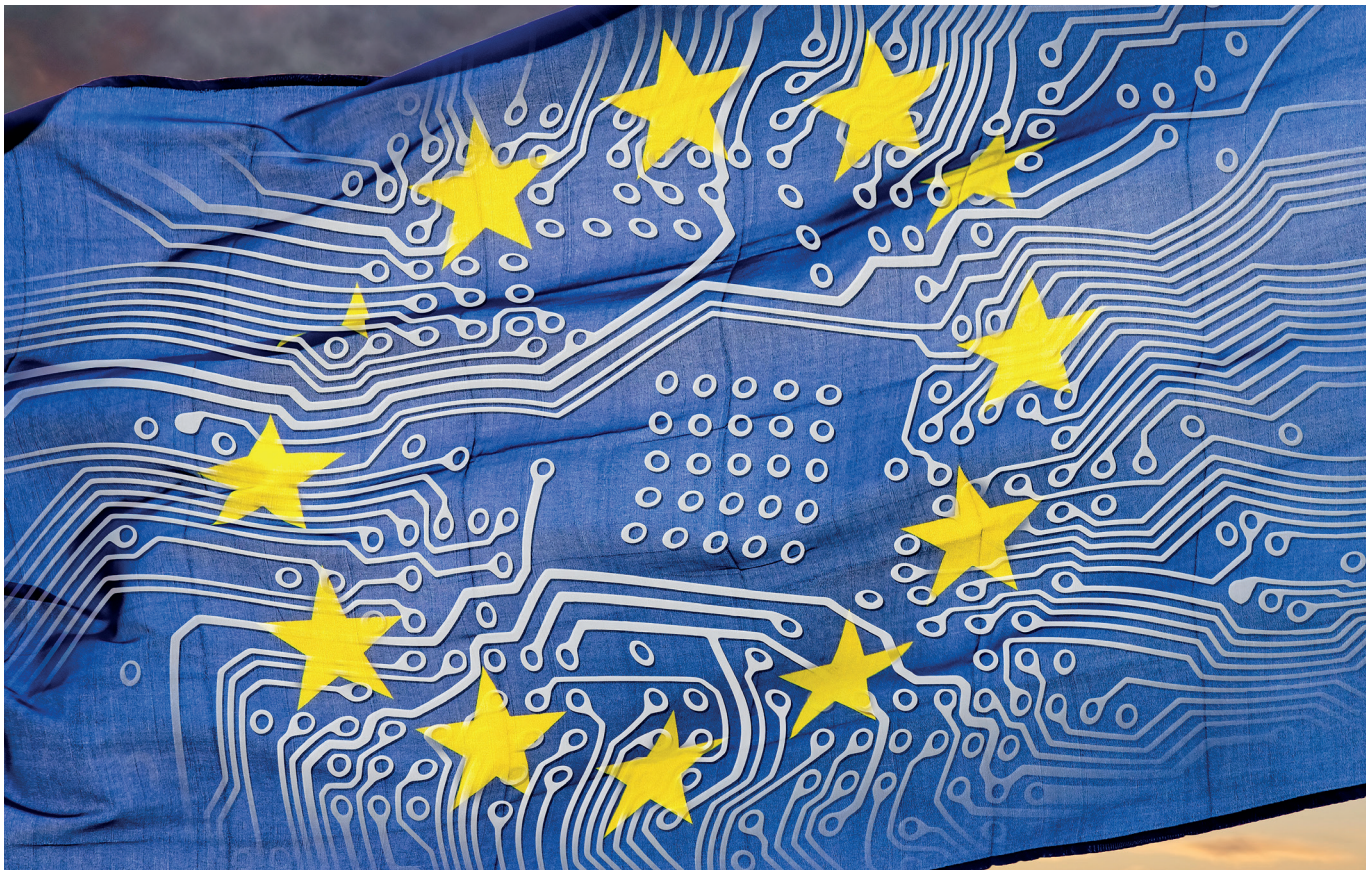
Newsletter IP/IT

September/Oktober 2022

Inhalt

Digitalisierungsvorhaben der EU

Der europäische Gesetzgeber hat sich im Zuge seiner Digitalstrategie zum Ziel gesetzt, die rechtlichen Vorgaben für die technische Entwicklung der vergangenen Jahre zu schaffen. Eine Vielzahl komplexer neuer Gesetzesvorhaben ist die Folge. Wir zeigen in einem kurzen Überblick, worum es bei den zentralen Gesetzesvorhaben der EU zur Digitalisierung geht.



E-Commerce: Digital Services Act

In Bezug auf den E-Commerce sind der Digital Services Act (DSA), die Omnibus Richtlinie und die Digital Content Richtlinie (DID-RL) von Relevanz. Alle Gesetzesvorhaben stärken die Rechte der Verbraucher und schaffen einen rechtssicheren Raum.

- So enthält die Omnibus-RL vorvertragliche Informationspflichten für den Onlinehandel, z. B. müssen Preissenkungen zukünftig den vorherigen Gesamtpreis anzeigen.
- Der DSA richtet sich mit dem Ziel eines sicheren digitalen Raums gegen Hate-Speech und andere illegale Inhalte auf Internetplattformen.
- Die DID-RL bezweckt einen verbesserten Schutz des Verbrauchers im Bereich digitaler Produkte, etwa durch ein Recht zur Aktualisierung digitaler Produkte.

Der DSA tritt voraussichtlich im Herbst in Kraft. Er richtet sich vordergründig an Vermittlungsdienste wie YouTube. Anders als der DSA sind Omnibus- und DID-RL bereits in Kraft getreten. Sie richten sich potenziell an alle Unternehmer, die entsprechende Verträge mit Verbrauchern abschließen.

Datenrecht und Künstliche Intelligenz: Data (Governance) Act

In Zusammenhang mit Daten und künstlicher Intelligenz hat die EU insbesondere den Data Act (DA), den Data Governance Act (DGA), den Artificial Intelligence Act (AIA) und die Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (ePrivacyVO) auf den Weg gebracht.

- Der DA und der DGA bezwecken die Erschaffung eines EU-Binnenmarktes für Daten. Dafür regelt der DGA die gemeinsame Nutzung von Daten zwischen öffentlichem Sektor und Unternehmen sowie die Verfügbarkeit von Daten. Der DA soll ein Zugangsrecht der Nutzer zu nutzergenerierten Daten schaffen. Teil dieses Ziels ist es auch, dem Nutzer den Wechsel des Anbieters von Cloud-Diensten zu erleichtern.
- Die ePrivacyVO bezweckt, die Vertraulichkeit der elektronischen Kommunikation der Nutzer zu schützen.
- In unmittelbarem Zusammenhang zu diesen Vorhaben steht der AIA. Er zielt darauf ab, einen risikobasierten Regelungsrahmen für Künstliche Intelligenz (KI) zu schaffen. Je höher das Risiko durch die KI ist, desto umfangreicher sind die einschlägigen Regelungen des AIA gehalten.

Allerdings ist bislang nur der DGA in Kraft getreten, wohingegen der Zeitpunkt des Inkrafttretens von DA und AIA noch offen ist.

Kartellrecht: Digital Market Act

Der Digital Market Act (DMA) erfasst die kartellrechtlichen Bezüge der Digitalisierung. Er ergänzt das Wettbewerbsrecht und beschränkt die Position marktbeherrschender Digitalkonzerne (wie Google und Facebook), wodurch ihm besondere Bedeutung für die Digitalstrategie zukommt. Denn nur die Regulierung dieser Akteure gewährleistet, dass auch andere Akteure durch die Nutzung von Daten innovativ neue Geschäftsmodelle entwickeln können. So sollen zukünftig Suchmaschinen beim Ranking daran gehindert sein, eigene Angebote zu bevorzugen. Betroffen von diesem noch im Entwurfsstadium befindlichen Vorhaben sind entsprechend ausgesuchte Digitalkonzerne. Der DMA tritt voraussichtlich (wie der DSA) im Herbst diesen Jahres in Kraft.

IT-Sicherheit: NIS2-RL und DORA

Je umfassender und intensiver digitale Geschäftsmodelle und die Digitalisierung unser Leben und unseren Alltag bestimmen, desto stärker muss die Integrität der virtuellen Umgebung durch angemessene IT-Standards gesichert sein. Im Hinblick auf kritische Infrastrukturen gab es dazu bereits in der Vergangenheit die NIS-RL. Nach erster Überprüfung der NIS-RL auf ihre Effektivität hat die EU die NIS2-RL vorgeschlagen, um so fortbestehende Lücken auszubessern. Ebenso hat sie mit dem Digital Operational Resilience Act (DORA) ein weiteres Vorhaben auf den Weg gebracht, dass eine hinreichende IT-Sicherheit im Finanzsektor gewährleisten soll. Anders als die NIS2-RL soll die DORA alle Wirtschaftsakteure im Finanzsektor (wahrscheinlich auch jegliche IT-Dienstleister) ansprechen.

Microsoft 365: Die datenschutzrechtlichen Voraussetzungen für den rechtskonformen Einsatz

Die Nutzung von Microsoft 365 bringt sowohl datenschutzrechtliche als auch betriebsverfassungsrechtliche Themen mit sich. Als technische Einrichtung, die die Überwachung von Leistung und Verhalten der Arbeitnehmer ermöglicht, unterliegt die Einführung und Nutzung der Mitbestimmung des Betriebsrats. Das Bundesarbeitsgericht hat nun klargestellt, dass die unternehmenseinheitliche Nutzung von Microsoft 365 die Zuständigkeit des Gesamtbetriebsrats (GBR) begründet. Zudem muss die Datenschutzgrundverordnung (DSGVO) beachtet werden, auch diesbezüglich gibt es Neues:

Voraussetzungen der Zuständigkeit des GBR

Das BAG hatte sich in seinem Beschluss vom 08.03.2022 (1 ABR 20/21) mit der Frage zu beschäftigten, ob hinsichtlich der betrieblichen Mitbestimmung bei der Einführung und Anwendung des Softwarepakets Microsoft 365 (damals noch „Office 365“) die Zuständigkeit des Betriebsrats oder des GBR eröffnet ist, wenn das Softwarepaket unternehmensweit eingesetzt werden soll. Während die Einordnung als „technische Einrichtung“ im Sinne des § 87 Abs. 1 Nr. 6 BetrVG, die die Überwachung von Verhalten und Leistung der Arbeitnehmer theoretisch ermöglicht, unproblematisch war, fühlte sich der antragstellende lokale Betriebsrat bei der Mitbestimmung übergangen. Dieser war der Ansicht, er habe zumindest bei Teilen des Softwarepakets mitzubestimmen, denn die zentralen Administrationsrechte könnten (jedenfalls für einige Module) auf betrieblicher Ebene geregelt und die Anwendung in den einzelnen Betrieben unterschiedlich ausgestaltet werden. Mithin bestünde keine zwingende technische Notwendigkeit für eine unternehmensweit einheitliche Regelung, sodass die Zuständigkeit des GBR nach § 50 Abs. 1 S. 1 BetrVG nicht eröffnet sei.

Die „1-Tenant-Lösung“ von Microsoft 365

Dieser Ansicht folgte das Gericht jedoch nicht. Voraussetzung der Zuständigkeit des GBR nach § 50 Abs. 1 S. 1 BetrVG sei zum einen, dass es sich um eine mehrere Betriebe betreffende Angelegenheit handle und zum anderen objektiv ein zwingendes Erfordernis für eine unternehmenseinheitliche oder betriebsübergreifende Regelung bestehe. Entscheidend sei dabei der Inhalt und Zweck des Mitbestimmungstatbestands, der einer zu regelnden Angelegenheit zugrunde liegt. Insbesondere nicht ausreichend sei allein der Wunsch des Arbeitgebers nach einer unternehmenseinheitlichen oder betriebsübergreifenden Regelung, sein Kosten- oder Koordinierungsinteresse sowie reine Zweckmäßigkeitsgesichtspunkte. Das zwingende Erfordernis für eine unternehmenseinheitliche Regelung sah das BAG im entschiedenen Fall darin, dass es sich um eine sog. „1-Tenant-Lösung“ handelte, bei der die Administrationsrechte zentral vergeben werden. Maßgeblich für die Zuständigkeit des GBR sei mithin, dass durch die zentralen Administrationsrechte auch eine zentrale, unternehmensübergreifende Überwachungsmöglichkeit bestehe. Dass bei einzelnen Modulen benutzerbezogene Einstellungen vor-

genommen werden können, führe hingegen nicht zu einer anderen Bewertung, da die zur Leistungs- und Verhaltenskontrolle geeigneten Komponenten oder Funktionen nicht auf bestimmte Personen oder Personengruppen einschränkbar seien. Auch handle es sich um eine einheitliche betriebsverfassungsrechtliche Angelegenheit, sodass eine Aufspaltung der Zuständigkeit von Betriebsrat und GBR für einzelne Module des Softwarepakets bzw. für die Einführung einerseits und die Anwendung andererseits nicht in Frage komme.

Mitbestimmung auch bezüglich „des Datenschutzes“?

Die Entscheidung des Gerichts führt zu einer erfreulichen Klarstellung im Hinblick auf die Zuständigkeitsverteilung von Betriebs- und GBR. Dies ist insbesondere wegen der weiten Verbreitung von Microsoft 365 in Unternehmen und Betrieben von enormer Praxisrelevanz. Der Einsatz von Microsoft 365 hat in der jüngeren Vergangenheit erhebliche datenschutzrechtliche Bedenken hervorgerufen. Aus Sicht des Betriebsrats stellt sich insofern die Frage, ob dieser mittels des Mitbestimmungsrechts auch auf Fragen des Datenschutzes Einfluss nehmen kann. Diesbezüglich gilt zunächst, dass dem Betriebsrat kein Mitbestimmungsrecht hinsichtlich „des Datenschutzes“ zusteht. Ein solches ergibt sich erst über einen der Tatbestände des § 87 Abs. 1 BetrVG, im Falle von Microsoft 365 eben über § 87 Abs. 1 Nr. 6 BetrVG. Insofern kann der (Gesamt-)Betriebsrat die Ausgestaltung des Datenschutzes doch beeinflussen.

Entwicklungen im Hinblick auf die Drittstaatenübermittlung

Aus unternehmerischer Sicht ist der Einsatz von Microsoft 365 vor allem wegen der möglichen Übermittlung personenbezogener in die USA problematisch. Die USA ist nach dem Scheitern des EU-US-Privacy-Shields als unsicheres Drittland im Sinne der DSGVO einzustufen, sodass die Datenübermittlung durch geeignete Mechanismen gesichert werden muss, insbesondere um den drohenden Zugriff durch die US-Geheimdienste zu verhindern. Microsoft ist diesbezüglich im ständigen Austausch mit den deutschen und europäischen Aufsichtsbehörden. Zwischenzeitlich wurde angekündigt, dass ab Ende 2022 eine Verarbeitung der in den Cloud-Diensten gespeicherten Daten nur noch in Europa erfolgen soll. Außerdem arbeiten die EU und die USA weiterhin an einem Nachfolgeabkommen für das EU-US-Privacy-Shield, welches die Datenübermittlung erheblich vereinfachen würde.

Einsatz von Microsoft 365 an Schulen

Die Fortschritte im Hinblick auf die Drittstaatenproblematik gestalten sich jedoch zäh, sodass einzelne Aufsichtsbehörden jedenfalls bezüglich des Einsatzes von Microsoft 365 in Schulen die Initiative ergreifen. Den Anfang machte bereits 2019 der Hessische Datenschutzbeauftragte, der zunächst den Einsatz als datenschutzrechtlich unzulässig bewertete, nach Gesprächen mit Microsoft aber nur einen Monat später erklärte, die Nutzung unter bestimmten Voraussetzungen und dem Vorbehalt weiterer Prüfungen vorläufig zu dulden. Der LfDI des Landes Baden-Württemberg betreute zwischen Herbst 2020 und Frühling 2021 ein Pilotprojekt, in dem in Zusammenarbeit mit Microsoft anhand einer funktionell eingeschränkten und möglichst datenschutzkonformen Konfiguration von Microsoft 365 überprüft wurde, ob ein datenschutzkonformer Einsatz an Schulen möglich ist. Trotz des Abschaltens von Funktionen, die aus datenschutzrechtlicher Sicht als besonders bedenklich eingestuft wurden, kam der LfDI zu dem Ergebnis, dass der Einsatz ein sehr hohes Risiko mit sich bringe. Aus diesem Grund wurde empfohlen, auf andere, datenschutzkonforme digitale Bildungsplattformen zurückzugreifen. Diese Empfehlung wurde jüngst in eine Aufforderung an die Schulen in Baden-Württemberg umgewandelt, entweder die Nutzung von Microsoft 365 zu beenden oder den datenschutzkonformen Betrieb eindeutig nachzuweisen. Dass ein datenschutzkonformer Betrieb möglich ist, davon scheint auch der rheinland-pfälzische LfDI – trotz Bedenken – auszugehen. Jedenfalls hat dieser in einem FAQ zu Microsoft 365 Hinweise darauf veröffentlicht, unter welchen Voraussetzungen ein Einsatz von Microsoft 365 an Schulen datenschutzrechtlich zulässig sein kann.

Voraussetzungen für einen datenschutzkonformen Einsatz

Auch wenn sich die dortigen Darstellungen auf den Einsatz an Schulen fokussieren, lassen sich diese auch auf die Nutzung durch Unternehmen übertragen. Um dem Risiko des Zugriffs durch US-Geheimdienste zu begegnen, sollte eine „on-Premises-Lösung“ verwendet werden, bei der Microsoft 365 entweder auf eigenen oder aber auf IT-Strukturen von Anbietern betrieben wird, die die Daten innerhalb der EU/des EWR speichern und nicht dem US-amerikanischen Recht unterliegen. Im Hinblick auf die durch Microsoft erhobenen Telemetrie-Daten sollte deren Übertragung durch entsprechende Einstellungen in Microsoft 365 bzw. dem Betriebssystem so weit wie möglich unterbunden werden. Wo dies nicht möglich ist, sollten die Daten durch eine geeignete Firewall „gefiltert“ werden, sodass eine Übertragung nicht stattfindet. Dabei ist zu beach-

ten, dass dieser Vorgang mit funktionalen Einschränkungen verbunden sein kann. Als weitere Maßnahmen kommen etwa die Nutzung vorkonfigurierter und abgesicherter Browser mit integrierten Schutzmaßnahmen sowie die Zwischenschaltung entsprechend vorkonfigurierter Terminal-Clients zur weitestgehenden Anonymisierung/Gleichschaltung der Metadaten, die Verwendung datensparsam konfigurierter Endgeräte, die Verwendung dienstlicher pseudonymer Mailadressen/Accounts und das Verbot der Nutzung privater Microsoft Accounts sowie die Umleitung des Internetverkehrs über eine eigene Infrastruktur mit geeigneten technischen Maßnahmen zur Verschleierung der heimischen IP-Adressen in Betracht.

Ergänzt werden diese Maßnahmen durch die Verwendung der sog. EU-Standard-Datenschutzklauseln. Diesbezüglich ist jedoch zu beachten, dass der EuGH für die Übermittlung in die USA zusätzliche Maßnahmen für erforderlich hält, die sicherstellen, dass ein im Wesentlichen gleichwertiges Schutzniveau wie in der EU gewährleistet wird. Weil jedoch individuelle Vereinbarungen mit Microsoft kaum abzuschließen sind, bleibt Unternehmen bis auf weiteres nur, durch entsprechende Voreinstellungen und die Implementierung technischer und organisatorischer Maßnahmen selbst für einen höheren Schutz der verarbeiteten Daten zu sorgen. Des Weiteren sollten auch die mit Microsoft geschlossenen Verträge überprüft und erforderlichenfalls neu verhandelt werden. Eine Überprüfung ist auch dahingehend erforderlich, ob eine Datenschutz-Folgeabschätzung durchzuführen ist. Im Hinblick auf die eigenen Mitarbeiter sind schließlich die Erfüllung der Informationspflichten und etwaige Schulungserfordernisse zu beachten.

Microsoft Teams als „interpersoneller Telekommunikationsdienst“

Seit dem 1. Dezember 2021 gelten die neuen Regelungen im Telekommunikationsgesetz (TKG). Telekommunikationsdienste im Sinne des Gesetzes (§ 3 Rn. 61 lit. b TKG) sind nunmehr auch sog. interpersonelle Telekommunikationsdienste (§ 3 Rn. 24 TKG) als gewöhnlich gegen Entgelt erbrachte Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglichen, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind. Der LDI NRW hat nun in einer Handreichung zu Online-Prüfungen an Hochschulen erstmals festgestellt, dass Videokonferenzdienste – und damit etwa auch Microsoft Teams – als interpersoneller Telekommunikationsdienst im vorgenannten Sinne einzustufen seien. Eine solche Einordnung hat zur Folge, dass der Anbieter des Telekommunikationsdienstes, in diesem Fall also Microsoft, als Telekommunikationsanbieter anzusehen wäre und somit auch dem Fernmeldegeheimnis (§ 3 Abs. 2 S. 1 Nr. 2 TTDSG) unterfallen würde. Zuständige Aufsichtsbehörde wäre der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (§ 29 Abs. 1 TTDSG).

Auch wenn Unternehmen als Nutzer eines Videokonferenzdienstes nicht als Telekommunikationsanbieter anzusehen sind (dies ist weiterhin umstritten), brächte eine entsprechende Einstufung von Microsoft auch für diese Prüfungsbedarf mit sich. Dieser liegt darin begründet, dass sich Microsoft in diesem Falle nicht mehr darauf berufen könnte, bei der Nutzung von Microsoft Teams lediglich als Auftragsverarbeiter tätig zu werden. Dies hat zur Folge, dass in den datenschutzrechtlichen Dokumentationen die Übermittlung personenbezogener Daten (in Form von Metadaten, also z. B. IP-Adressen, die übertragene Datenmenge, der Browsertyp, das Betriebssystem und Informationen darüber, wer wann mit wem kommuniziert, aber auch die technischen Übertragungsdaten in Bezug auf den Transport der Inhaltsdaten) an Microsoft als Telekommunikationsanbieter und somit datenschutzrechtlich Verantwortlichen dargestellt werden muss. Dies betrifft etwa die erstellten Verarbeitungsverzeichnisse, die Informationspflichten für die Beschäftigten, Kunden und Businesspartner, sowie auch die Formulierungen in Betriebsvereinbarungen.

Schwierigkeiten würden sich auch im Hinblick auf die vertraglichen Vereinbarungen mit Microsoft ergeben. Der LDI NRW geht davon aus, dass das Unternehmen als die den Videokonferenzdienst nutzende Stelle gemäß Art. 32 DSGVO zur Gewährleistung technischer und organisatorischer Maßnahmen für die Sicherheit der Verarbeitung der Inhaltsdaten verpflichtet ist. Aus dieser Verpflichtung schließt die Behörde, dass diesbezüglich entsprechende Klauseln in den Vertrag mit dem Anbieter von Telekommunikationsdiensten aufzunehmen seien. Aus der Vergangenheit ist jedoch bekannt, dass allenfalls Big Player dazu in der Lage sind, mit Microsoft einzelne Vertragsdetails auszuhandeln, sodass fraglich ist, wie einer solchen Verpflichtung nachgekommen werden könnte. Auch insofern bleiben die weiteren Entwicklungen, auch in Form von weiteren aufsichtsbehördlichen Stellungnahmen, zu beobachten.

Der Anspruch auf immateriellen Schadensersatz nach der DSGVO vor dem EuGH

Hintergrund

Die Belastung mit einem Bußgeld ist eine bekannte Sorge in Zusammenhang mit Datenschutzverstößen nach der Datenschutzgrundverordnung (DSGVO). Mittlerweile findet ein weiterer Sanktionsmechanismus vermehrt Beachtung: der Schadensersatzanspruch einer Privatperson.

So haben in den letzten Jahren vermehrt Privatpersonen mit ihren auf Zahlung eines immateriellen Schadensersatz gerichteten Klagen vor den ordentlichen Gerichten Erfolg. Diese Klagen werfen offene Fragen zur Auslegung der DSGVO auf, über die voraussichtlich bald der Europäische Gerichtshof (EuGH) entscheiden muss.

Auf den Punkt

Zahlreiche Gerichte, z.B. das Amtsgericht Hagen, das Landgericht Saarbrücken und der Oberste Gerichtshof Österreichs, haben sich in Vorabentscheidungsersuchen an den Europäischen Gerichtshof mit Fragen zu den Voraussetzungen des datenschutzrechtlichen Schadensersatzanspruchs nach Art. 82 DSGVO gewandt.

Die Antworten des EuGH sind im Hinblick auf eine divergierende Rechtsprechung (restriktive vs. weite Auslegung des Art. 82 DSGVO) dringend notwendig und vermögen den Streit um die Frage zu beenden, ob für einen immateriellen Schaden bereits jeder Verstoß gegen die DSGVO ausreicht oder ob die Rechtsverletzung von zumindest einigem Gewicht sein muss (sog. Erheblichkeitsschwelle).

Sachverhalt

Das AG Hagen (Rechtssache C-687/21) möchte insbesondere wissen, ob es für einen Schadensersatzanspruch erforderlich ist, dass außer der unberechtigten Bekanntgabe personenbezogener Daten an einen Dritten ein vom Anspruchssteller darzulegender immaterieller Schaden festzustellen ist (Vorlagefrage 2). Weiter fragt es den EuGH danach, ob das Unbehagen der betroffenen Person, deren personenbezogene Daten unbefugt an einen Dritten offen gelegt wurden, für einen immateriellen Schaden im Sinne des Art. 82 DSGVO genügt. Schließlich fragt es danach, ob die Zubilligung eines Ersatzes für einen immateriellen Schaden einen Strafcharakter hat (ähnlich einer Vertragsstrafe).

Der Oberste Gerichtshof Österreichs (Rechtssache C-300/21) fragt danach, ob für einen Schadensersatzanspruch nach Art. 82 DSGVO bereits die Verletzung von Bestimmungen der DSGVO ausreicht oder ob die betroffene Person zusätzlich einen Schaden erlitten haben muss. Mit seinen weiteren Fra-

gen möchte der Oberste Gerichtshof wissen, ob es für die Bemessung des Schadensersatzes neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts gibt und ob die Auffassung mit dem Unionsrecht vereinbar ist, dass Voraussetzung für den Zuspruch immateriellen Schadens ist, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht.

Das Landgericht Saarbrücken (C-741/21) möchte ebenfalls wissen, ob der Begriff des immateriellen Schadens so zu verstehen ist, dass er jede Beeinträchtigung der geschützten Rechtsposition erfasst, unabhängig von deren sonstigen Auswirkungen und deren Erheblichkeit.

Einordnung

Die Antworten des EuGH werden mit Spannung erwartet, da die Gerichte sich über die Auslegung von Art. 82 DSGVO nicht einig sind. Strittig ist, ob ein Bagatellverstoß für den Zuspruch eines Schadensersatzanspruchs ausreichend sei oder der Verstoß gegen die DSGVO eine gewisse Erheblichkeitsschwelle erreichen müsse.

Der entscheidende Aspekt ist die Auslegung des Begriffs des immateriellen Schadens. Hintergrund der Unsicherheiten ist die traditionelle Auffassung deutscher Gerichte, wonach die Zubilligung eines Geldentschädigungsanspruchs von einer besonders schweren Verletzung des Persönlichkeitsrechts abhängig zu machen ist.

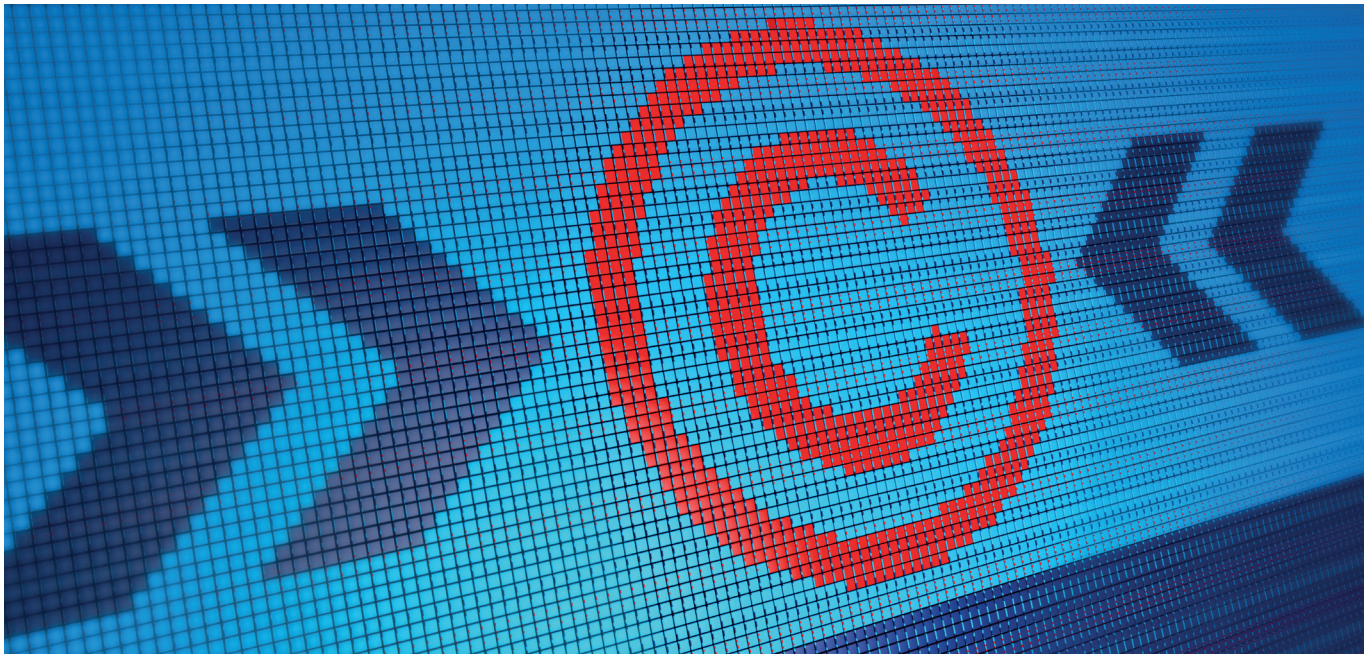
Mittlerweile gehen Gerichte zunehmend davon aus, dass weder eine spürbare Beeinträchtigung des Betroffenen noch das Überschreiten einer Erheblichkeitsschwelle notwendig ist, um einen Ausgleich in Geld zuzusprechen (vgl. z. B. LAG Hamm, Urteil vom 14.12.2021 – 17 Sa 1185/20; LAG Niedersachsen, Urteil vom 22.10.2021 – 16 Sa 761/20, anders OLG Dresden, Urteil vom 30.11.2021 – 4 U 1158/21). Vielmehr rückt das Ziel der Abschreckung stärker in den Vordergrund (vgl. OLG Dresden aaO.; LAG Hessen, Urteil vom 18.10.2021 – 16 Sa 380/20), das dem deutschen Schadensersatzrecht fremd ist.

Unser Kommentar

Die Entscheidung des EuGH ist nicht absehbar. Gewährt der EuGH dem europarechtlichen Gebot wirksamer Rechtsdurchsetzung europäischen Rechts („effet utile“) Vorrang, kann bereits jeder Verstoß gegen die DSGVO einen immateriellen Schaden der betroffenen Person darstellen. Auf die Spürbarkeit der Beeinträchtigung kommt es dann nicht mehr an.

Dies dürfte die Anstrengungen der Unternehmen zur Einhaltung der DSGVO verstärken. Entgegen den grundsätzlichen Wertungen des deutschen Zivilrechts stünde jeder betroffenen Person bei einem Verstoß gegen die DSGVO ein „Schmerzensgeld“ zu.

Die Verwirkung markenrechtlicher Ansprüche



Hintergrund

Der Inhaber einer prioritätsälteren Marke kann grundsätzlich nicht gegen die Benutzung einer prioritätsjüngeren Marke vorgehen, wenn er deren Benutzung während eines Zeitraums von fünf aufeinander folgenden Jahren in Kenntnis der Benutzung geduldet hat. In diesem Fall hat der Rechtsinhaber sein Recht durch Duldung verwirkt.

Der europäische Gerichtshof (EuGH) hat in einem aktuellen Urteil die Vorgaben an die Verwirkung markenrechtlicher Ansprüche konkretisiert.

Sachverhalt

Die Klägerin ist Inhaberin der prioritätsälteren Unionswortmarke „HEITEC“ sowie des gleichlautenden prioritätsälteren Unternehmensnamensbestandteils. Die Beklagte meldete im Jahr 2002 eine deutsche Wortbildmarke mit dem Wortbestandteil „heitech promotion“ an und firmiert seit 2003 unter der Bezeichnung „HEITECH Promotion GmbH“. Im Jahr 2008 meldete sie daneben eine Unionswortbildmarke mit dem Wortbestandteil „heitech“ an. Spätestens Ende 2004 erlangte die Klägerin von der Firmierung sowie der Benutzung der deutschen Marke der Beklagten Kenntnis. Im Juli 2008 erfuhr die Klägerin von der Anmeldung der Unionsmarke durch die Beklagte und hatte spätestens seit Mitte 2009 Kenntnis von der Benutzung dieses Zeichens.

Im Jahr 2009 mahnte die Klägerin die Beklagte u. a. wegen der Benutzung der Unionsmarke mit dem Wortbestandteil „heitech“ ab und reichte am 31. Dezember 2012 eine Verletzungsklage beim LG Nürnberg-Fürth ein. Die Klage konnte jedoch aufgrund mangelnder Sorgfalt der Klägerin bei der Prozessführung erst im Mai 2014 zugestellt werden.

Nach Durchlaufen des Instanzenzugs in Deutschland, legte der BGH dem EuGH die Angelegenheit im Rahmen eines Vorabentscheidungsverfahrens vor. Letzteres ist regelmäßig der Fall, wenn in einem nationalen Gerichtsverfahren nicht klar ist, wie Gemeinschaftsrecht – hier Art. 9 der Richtlinie 2008/95/EG sowie Art. 54, 110 und 111 der Verordnung EG Nr. 207/2009 – auszulegen ist. Der BGH wollte u. a. wissen,

- ob bereits eine Handlung wie etwa eine Abmahnung die Duldung beende;
- ob im Fall eines zwar vor Ablauf der Verwirkungsfrist eingelegten, aber aufgrund mangelnder Sorgfalt des Rechtsinhabers erst nach Ablauf der Verwirkungsfrist zugestellten gerichtlichen Rechtsbehelfs, die Verwirkung verhindert werde;
- ob sich die Verwirkung auch auf die Geltendmachung etwaiger Neben- oder Folgeansprüche wie z.B. Ansprüche auf Schadensersatz, Auskunft oder Vernichtung erstrecke.

Die Entscheidung

In seiner Entscheidung stellte der EuGH Folgendes klar:

- Allein eine Abmahnung, mit der sich der Inhaber einer prioritätsälteren Marke oder eines sonstigen prioritätsälteren Rechts der Benutzung einer prioritätsjüngeren Marke widersetzt, unterbricht nicht die fünfjährige Verwirkungsfrist. Vielmehr muss der Rechtsinhaber im Fall einer nicht zufriedenstellenden Reaktion auf die Abmahnung innerhalb einer angemessenen Frist weiter gegen die Verletzung seiner Rechte – ggfs. durch Einlegung eines behördlichen oder gerichtlichen Rechtsbehelfs – vorgehen, um die Verwirkungsfrist zu unterbrechen.
- Die Einlegung eines gerichtlichen Rechtsbehelfs, mit dem der Inhaber einer prioritätsälteren Marke oder eines sonstigen prioritätsälteren Rechts die Nichtigerklärung einer prioritätsjüngeren Marke begehrt oder sich deren Benutzung widersetzt, reicht zur Unterbrechung der fünfjährigen Verwirkungsfrist nicht aus, wenn die Erhebung zwar vor Ablauf der Verwirkungsfrist erfolgte, aber die vom Rechtsinhaber verursachten Zustellungsmängel erst nach Ablauf der Verwirkungsfrist behoben werden konnten.
- Die Verwirkung umfasst neben dem Anspruch auf Nichtigerklärung und Unterlassung auch Neben- oder Folgeansprüche (z. B. Ansprüche auf Schadensersatz, Auskunft oder auf Vernichtung von Waren).

Unser Praxishinweis

Mit Blick auf das vorgenannte Urteil sollte der Rechtsinhaber, der gegen die Benutzung einer prioritätsjüngeren Marke oder eines sonstigen prioritätsjüngeren Rechts vorgehen möchte, sicherstellen, dass er dies hinreichend erkennbar zum Ausdruck bringt. Andernfalls besteht das Risiko, dass er sein Recht verliert, gegen die Benutzung vorgehen zu können.

Daneben sollte die Entscheidung, nicht gegen die Benutzung einer prioritätsjüngeren Marke oder eines sonstigen prioritätsjüngeren Rechts vorzugehen, wohl überlegt sein. Schließlich erstreckt sich die Verwirkung nicht nur auf die in der Vergangenheit liegenden Unterlassungsansprüche nebst etwaiger Neben- oder Folgeansprüche, sondern auch auf etwaige auf die Zukunft gerichtete Ansprüche.

Der Relevanz der Entscheidung steht dabei nicht entgegen, dass die Richtlinie 2008/95/EG sowie die Verordnung EG Nr. 207/2009 mittlerweile außer Kraft getreten sind. Die Entscheidung ist auch auf die derzeit geltende Richtlinie (EU) 2015/2436 und Verordnung (EU) 2017/1001 übertragbar.

Studie von IBM Security: Datenschutzverstöße werden sowohl für Unternehmen als auch für Kunden teurer

Hintergrund

Bereits seit 17 Jahren veröffentlicht IBM Security die jährliche Studie „Cost of a Data Breach“, die sich mit der Entwicklung der Kosten beschäftigt, die für Datenschutzverstöße auf Unternehmensseite anfallen. Zu diesem Zweck wurden Daten aus 17 Ländern und 17 Industriezweigen analysiert. Das Ergebnis: Die Kosten für einen Datenschutzverstoß steigen nicht nur für Unternehmen. Auch für Kunden bedeutet dies Mehrkosten, da zahlreiche Unternehmen die entstandenen Kosten an diese weitergeben.

Kosten für Datenschutzverstöße steigen

Betrugen die durchschnittlichen Kosten für einen Datenschutzverstoß im Jahr 2020 noch USD 3,86 Mio., so seien laut der Studie im Jahr 2022 bereits Kosten in Höhe von USD 4,35 Mio. entstanden. In dem Zweijahreszeitraum sei mithin ein Anstieg von 12,7 % zu verzeichnen gewesen. Dabei ist zu beachten, dass die Studie nicht nur Daten aus Europa berücksichtigt und daher der Anstieg nicht allein durch das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) zu erklären ist. Gleichwohl wird der Anteil der DSGVO nicht un-

erheblich sein, da diese zur Verhängung von enormen Bußgeldern gegen Google (EUR 90 Mio.), WhatsApp (EUR 225 Mio.) oder Amazon (EUR 746 Mio.) geführt hat.

Mit diesem Anstieg einher gehen laut der Studie erhöhte Kosten für Produkte und Services auf Seiten der Kunden, da ganze 60 % der untersuchten Unternehmen ihre Preise aufgrund der gestiegenen Kosten für Datenschutzverstöße angehoben hätten.

Die häufigsten und teuersten Datenschutzverstöße

Ein Blick auf die „Top 3" der Datenschutzverstöße überrascht wenig: Häufigste Datenschutzverstöße, so die Studie, waren gestohlene oder kompromittierte Anmeldedaten (19 %), Phishing (16 %) sowie eine Fehlkonfiguration der Cloud (15 %). Hinsichtlich der Häufigkeit „nur" auf dem zweiten Platz, mittlerweile aber als teuerste Ursache etabliert, habe sich das sog. Phishing. Ein solcher Angriff auf die IT-Infrastruktur verursache durchschnittliche Kosten von USD 4,91 Mio.

Zugleich sei festgestellt worden, dass sich die Zahlung eines Lösegeld – etwa im Falle eine Ransomware-Attacke – für die betroffenen Unternehmen aus finanzieller Sicht wenig lohne. Zwar wiesen diese um USD 610.000 niedrigere durchschnittliche Kosten für einen Datenschutzverstoß auf, jedoch habe die durchschnittliche Lösegeldzahlung wiederum USD 812.000 betragen. Außerdem sei zu berücksichtigen, dass durch die Zahlung eines Lösegeldes ungewollt künftige Ransomware-Attacken finanziert werden. Im Falle einer Ransomware-Attacke sei vielmehr ein funktionierendes Incident-Response-Playbook (IR) entscheidend. Selbst wenn ein solches Sicherheitskonzept besteht, würde dieses aber von bis zu 37 % der Unternehmen nicht regelmäßig getestet.

Wiederkehrende Sicherheitsmängel

Ohnehin habe sich laut IBM Security gezeigt, dass die technischen Sicherheitsmaßnahmen bei vielen Unternehmen unzureichend seien. Dies liege schon darin begründet, dass zahlreiche Unternehmen nach eigener Auskunft nicht über ausreichend Sicherheitspersonal (62 %) verfügen. Ein solcher Mangel wirke sich direkt auf die durchschnittlichen Kosten für einen Datenschutzverstoß aus, fielen diese doch um durchschnittlich USD 550.000 niedriger aus, wenn ein Unternehmen nach eigenen Angaben über ausreichend Personal verfügt.

Des Weiteren sei zu beobachten, dass Unternehmen der kritischen Infrastruktur – etwa aus dem Finanzdienstleistungs-, Industrie-, Transport- und Gesundheitssektor – trotz Empfehlungen oftmals kein sog. Zero-Trust-Sicherheitsmodell implementiert hätten. Im Bereich der kritischen Infrastruktur würden laut Studie lediglich 21 % der Unternehmen eine solche risikobasierte Strategie nutzen. In anderen Bereichen sei der Anteil immerhin auf 41 % gestiegen. Dabei wirke sich ein Zero-Trust-Sicherheitsmodell insofern positiv auf die Kosten von Datenschutzverstößen aus, als dass diese im Durchschnitt um USD 1 Mio. sinken.

Ein weiteres wiederkehrendes Problem betreffe Sicherheitslücken in Clouds. Demnach befänden sich 43 % der untersuchten Unternehmen noch in einem frühen Stadium der Umsetzung von Sicherheitsmaßnahmen in ihren Cloudumgebungen oder hätten sogar noch gar nicht damit begonnen. Ein solcher Mangel wirke sich durchschnittlich in mehr als USD 660.000 höheren Kosten für Datenschutzverstöße aus.

Bedenklich sei zudem, dass 83 % der untersuchten Unternehmen während ihres Bestehens bereits mehr als einen Datenschutzverstoß erlebt haben. Dies verdeutliche die Zunahme von Cyberattacken, zeige aber zugleich die immer noch bestehenden Mängel in der IT-Sicherheit. Dies ist aus unternehmerischer Sicht auch deswegen problematisch, als dass fast 50 % der Kosten für Datenschutzverstöße erst mehr als ein Jahr nach dem Vorfall anfielen, was die finanzielle Planung deutlich erschwert.

Identifizierung kostenschonender Sicherheitsmaßnahmen

Die Studie identifizierte die Verwendung einer Hybrid-Cloud-Umgebung als vorteilhaft gegenüber einem reinen Public- oder Private-Cloud-Modell. Während bei der Nutzung einer Hybrid-Cloud-Umgebung im Falle von Datenschutzverstößen durchschnittlich Kosten in Höhe von USD 3,8 Mio. entstanden, betrugen diese bei einer reinen Public- oder Private-Cloud USD 5,02 Mio. bzw. USD 4,24 Mio.. Dies sei auch dadurch begründet, dass die Anwender einer Hybrid-Cloud in der Lage seien, Datenschutzverletzungen durchschnittlich 15 Tage früher zu erkennen und einzudämmen als der globale Durchschnitt, der 277 Tage benötigte.

Eine weitere kostenschonende Maßnahme stelle laut Studie die Nutzung einer sog. XDR-Technologie (Extended detection and response) dar. Bei Unternehmen, die diese Technologie verwendeten, verkürzte sich die Zeit zur Erkennung und Eindämmung von Datenschutzverstößen um durchschnittlich einen Monat im Vergleich zu Unternehmen, die XDR nicht implementiert haben.

Schließlich könne der Einsatz Künstlicher Intelligenz (KI) im IT-Sicherheitsbereich für die größte Kostenreduzierung auf Unternehmensseite sorgen. So habe die Datenauswertung ergeben, dass Unternehmen mit entsprechender KI ein Datenschutzverstoß durchschnittlich bis zu USD 3,05 Mio. weniger kostete als Unternehmen, die keine KI einsetzen.

Fazit

Die veröffentlichte Studie zeigt eindrücklich, dass zu viele Unternehmen das Thema IT-Sicherheit noch immer nicht ernst genug nehmen. Cyber-Attacken nehmen stetig zu, und werden Unternehmen ohne ausreichende IT-Sicherheit von ihnen getroffen, kann dies nicht nur in empfindlichen behördlichen Bußgeldern oder Schadensersatzansprüchen resultieren. Durch Ransomware-Attacken können ganze Unternehmen lahmgelegt werden, und der Image-Schaden in diesen Fällen ist immens. So zeit- und kostenintensiv die Implementierung von IT-Sicherheitsmaßnahmen und Datenschutz-Modellen auch sein mag, wird es doch Zeit, dass sich die Erkenntnis durchsetzt, dass ein proaktiver Schutz im Endeffekt kostengünstiger ist.

Hotelbewertungen

Einleitung

Der BGH hat in seinem aktuellen Urteil vom 09.08.2022 (Aktenzeichen VI ZR 1244/20) die Rechte von Hotels gegen anonyme Bewertungen auf Online-Reiseportalen gestärkt. Konkret hat sich der BGH mit den Nachweisanforderungen an den tatsächlichen Gästekontakt auseinandergesetzt. Demnach reicht grundsätzlich die Rüge des fehlenden Gästekontakts durch das bewertete Hotel aus, um eine Prüfpflicht des Bewertungsportals auszulösen. Der BGH trägt damit dem Umstand Rechnung, dass das bewertete Unternehmen die Angaben in der Regel nicht selbst überprüfen kann.

Hintergrund

Hotelbewertungen auf Reiseportalen stellen ein entscheidendes Kriterium bei der Auswahl der geeigneten Unterkunft dar. Sie geben Auskunft über die Zimmer, die Hotelanlage, den Service und die Gastronomie. Neben der Bewertung einzelner Kategorien anhand einer Punkteskala besteht die Möglichkeit einer individuell verfassten Bewertung in Textform. Zudem verschafft die Einordnung des Bewertenden in eine bestimmte Alterskategorie und Urlaubsform (z. B. Familienurlaub) einen Eindruck von den Anforderungen des Bewertenden.

Verfahren

Der Kläger des Verfahrens, ein Ferienpark an der Ostsee mit rund 4.000 Betten, hatte ein Reiseportal wegen negativer Bewertungen auf Unterlassung in Anspruch genommen. Er hat behauptet, die Bewertungen würden nicht von tatsächlichen Gästen seiner Anlage stammen und sich gleichzeitig negativ auf seine wirtschaftliche Tätigkeit auswirken. Eine negative Bewertung durch Konkurrenten sei nicht auszuschließen. Der Kläger selbst könne aufgrund der Pseudonymisierung jedenfalls nicht nachvollziehen, ob ein tatsächlicher Gästekontakt bestand.

Die Beklagte betreibt ein Reiseportal im Internet. Dort können Nutzer nach einer Registrierung mit einer E-Mail-Adresse Hotels buchen und diese bewerten. Die Bewertungen werden dann unter dem registrierten Namen des Nutzers veröffentlicht. Dabei ist es möglich, dass die Bewertungen pseudonymisiert oder anonym abgegeben werden. Bei bis zu zehn veröffentlichten Hotelbewertungen pro Monat erhalten die Nutzer Flugmeilen als Prämie. Die Beklagte hat auf Nachfrage der Klägerin jede Nachfrage bei Ihren Nutzern abgelehnt.

Entscheidung

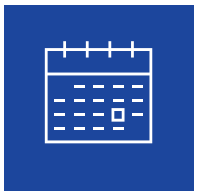
Der BGH entschied zugunsten des Klägers und kam in seinem Urteil zu folgendem Ergebnis:

- Der Unterlassungsanspruch ist nicht über die Haftungsprivilegierung gemäß § 10 Telemediengesetz (TMG) ausgeschlossen. Die Haftungsprivilegierung gilt nämlich nicht für Unterlassungsansprüche, deren Ursprung in einer vorangegangenen Rechtsverletzung liegt.
- Das Reiseportal ist als mittelbarer Störer verantwortlich, indem sie durch die Verletzung ihrer Prüfpflichten zur Beeinträchtigung des Rechtsguts willentlich und adäquat kausal beigetragen hat. Eine anlasslose Pflicht zur Überprüfung jedes einzelnen Nutzerbeitrags besteht zwar nicht. Wenn das betroffene Hotel die Bewertung jedoch mit der Begründung rügt, ein tatsächlicher Gästekontakt liege nicht vor, dann entsteht regelmäßig eine anlassbezogene Prüfpflicht des Bewertungsportals. Eine über diese Rüge hinausgehende Begründung ist zudem in den Fällen erforderlich, in denen sich die Identität der bewertenden Person unmittelbar aus der Bewertung ergibt.
- Bei der Frage nach den konkret erforderlichen Überprüfungsmaßnahmen des Portals muss berücksichtigt werden, dass solche Portale grundsätzlich rechtlich zulässig und vom Markt gewünscht sind. Der erforderliche Prüfaufwand darf deshalb den Betrieb des Portals weder wirtschaftlich gefährden noch unverhältnismäßig erschweren.
- Wenn der gerügten Bewertung kein Gästekontakt zugrunde liegt, führt dies zu einer Verletzung des Unternehmenspersönlichkeitsrechts des bewerteten Hotels.
- Erhält ein Portalbetreiber eine Rüge, obliegt ihm die Pflicht zur Prüfung des gerügten Beitrags innerhalb einer angemessenen Frist. Liegt tatsächlich eine Rechtsverletzung vor, muss der Portalbetreiber den Beitrag löschen (sog. „notice and take down“).
- Erfolgt nach Beanstandung durch das bewertete Hotel und Weiterleitung dieser Beanstandung durch das Reiseportal an die bewertende Person innerhalb einer angemessenen Frist keine Antwort, ist auch dann von einer berechtigten Beanstandung auszugehen. Diese hat zur Folge, dass auch in diesem Fall das Reiseportal den beanstandeten Eintrag löschen muss.

Ausblick

Der BGH hat sich in seinem Urteil mit den Prüfpflichten eines Portalbetreibers beschäftigt. Die dargelegten Gründe sind allgemeiner Natur. Es ist zu erwarten, dass die Rechtsprechung dieser Argumentationslinie bei sämtlichen Bewertungsportalen folgt. Bewertungsportale können der anlassbezogenen Prüfpflicht zuvorkommen, indem sie bei der Eingabe der Bewertung zusätzliche Daten abfragen. Eine solche Abfrage wird jedoch regelmäßig den Klarnamen erfordern und stellt daher die Verarbeitung personenbezogener Daten dar. Insofern sollte die Umstellung des Bewertungsportals datenschutzrechtlich begleitet werden. Keine Änderung ergibt sich für die Portale, die ohnehin die Möglichkeit einer Bewertung technisch davon abhängig machen, dass die bewertende Person auch tatsächlich die Unterkunft gebucht und dort übernachtet hat.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: iStockphoto/ismagilov: Seite 1; AdobeStock/gopixa: Seite 3; AdobeStock/suphakit73 : Seite 5; AdobeStock/Murrstock: Seite 8; iStockphoto/fatido: Seite 10; AdobeStock/lassedesignen: Seite 13

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS