Luther.

Newsletter IP/IT

1. Ausgabe 2020

Inhalt

Rechtliche Auswirkungen des Coronavirus auf IT-Unternehmen

Das Coronavirus kann erhebliche Auswirkungen auf den Geschäftsbetrieb von Unternehmen haben. Sowohl interne als auch externe Faktoren sind zu beachten, sodass eine solide rechtliche Absicherung zu empfehlen ist. Unternehmen müssen dabei nicht nur deutsches Arbeits- und Vertragsrecht, sondern wegen der Lieferketten ggf. auch lokales chinesisches Recht beachten.

Hintergrund

Das Coronavirus hat trotz aller Quarantäne- und Eindämmungsmaßnahmen mittlerweile Europa erreicht. Daher betreffen die Gefahren und Konsequenzen nicht mehr nur China, sondern haben globale Auswirkungen – und das nicht nur gesundheitlich, sondern auch in Bezug auf die Wirtschaft. Insbesondere IT-Unternehmen sind aufgrund ihrer naturgegebenen weltweiten Vernetzung besonders anfällig für die Auswirkungen des Coronavirus. Denn viele Unternehmen in der IT- und Kommunikationsbranche unterhalten Beziehungen zu Kunden und Lieferanten im asiatischen Raum, deren Geschäft durch die Epidemie stark eingeschränkt ist. Laut einer aktuellen Umfrage des Digitalverbands Bitkom rechnet daher jede vierte deutsche IT-Firma damit, dass das neuartige Virus zu Umsatzrückgängen im Jahr 2020 führen wird.

IT-Unternehmen sind daher gut beraten, sich mit möglichen wirtschaftlichen und rechtlichen Auswirkungen zu beschäftigen und sich auf Risiken und Konsequenzen in Verbindung mit dem Coronavirus vorzubereiten. Umfassende und branchenübergreifende Informationen zu den Auswirkungen des Coronavirus sowie eine komplexe Zusammenstellung insbesondere einschlägiger chinesischer Gesetze und Dekrete finden Sie auf unserer eigens erstellten, auch auf Englisch verfügbaren Infoseite: „Corona Virus: Rechtliche Auswirkungen auf Unternehmen“. Die arbeitsrechtlichen Implikationen – u. a. hinsichtlich mobilem Arbeiten, Zahlungsansprüchen und Kurzarbeit – greifen wir in unserem Sondernewsletter „COVID-19 trifft auf HR – Guideline für Arbeitgeber“ auf.

Mögliche Rechtliche Auswirkungen auf IT-Unternehmen

Ebenso wie der Mensch unterschiedliche Symptome als Reaktion auf eine Coronainfektion entwickelt, können auch unterschiedliche Bereiche eines IT-Unternehmens von den Auswirkungen des Virus betroffen sein. Und zwar sowohl im eigenen Betrieb als auch hinsichtlich externer Faktoren. Es lohnt sich daher, diejenigen Aspekte und Unternehmensberei-

che zu identifizieren, die typischerweise von den Auswirkungen einer solchen Epidemie betroffen sein können. Nur so lässt sich ein Ansatz für eine Präventions- und Deeskalationsstrategie konzipieren.

Auswirkungen im eigenen (deutschen/ europäischen) Unternehmen

Hier sind in erster Linie unmittelbare (einzelne) Erkrankungen in der eigenen Belegschaft denkbar, beispielsweise bei global agierenden IT-Dienstleistern, deren Mitarbeiter sich im Rahmen einer Entsendung zum Kunden in China infiziert haben. Ist ein solches Szenario bei Ihnen wahrscheinlich, sollten Präventions- und Deeskalationsmechanismen existieren. Dazu gehören interne und externe (zu lokalen Behörden/Gesundheitsbehörden) Meldewege und HR-Maßnahmen zur Fürsorge für die betroffenen Mitarbeiter (Vergütungsregelung bei Boni, ggf. zusätzliche Alimentierung für die Betroffenen und ggf. Angehörigen) sowie die Reaktion auf etwaige Quarantäneauflagen. Darüber hinaus sollten sich Unternehmen über vorhandenes qualifiziertes Ersatzpersonal vergewissern.

Je nach eigenem Gefährdungsgrad des Unternehmens muss auch ein möglicher „worst case“ gedanklich exerziert werden: Was ist zu tun, wenn ganze Belegschaftsteile oder Abteilungen betroffen sind? Für einen solchen Fall müssen über die bereits genannten Maßnahmen hinaus Notfallpläne für die Kompensation von Produktions- und Dienstleistungsengpässen existieren. Aus rechtlicher Sicht sollte ein Überblick über die bestehenden vertraglichen Pflichten vorhanden sein, deren Nicht-, Schlecht- oder Späterfüllung droht. Dazu gehören Fristen, denen die eigene Leistung unterliegt, Kenntnis über etwaige Vertragsstrafen und die Evaluierung möglicher „Reißleinen“ (Störung der Geschäftsgrundlage, Force Majeure, außerordentliche Kündigung). Dies kann nur durch ein effektives Vertragsmanagement gelingen.

Auswirkungen bei eigenen Niederlassungen, Filialen etc. in China

Unternehmen müssen sich auch bei Auswirkungen in Auslandsniederlassungen Gedanken zur Reaktion auf Erkrankungen in der eigenen Belegschaft sowie zur Übersicht über die eigenen Verpflichtungen machen. Hier treten die Besonderheiten des chinesischen Rechtsraums hinzu. Es ist daher elementar, auch in der deutschen/europäischen Zentrale einen Überblick über die rechtliche Situation in den betroffenen chinesischen Gebieten zu haben, in denen das Unternehmen eigene Standorte besitzt. In China sind binnen kürzester Zeit seit Entdeckung des Coronavirus dutzende nationale und provinzbezogene, behördliche und gesetzliche Regelungen erlassen worden, deren Beachtung verbindlich ist. Diese Regelungen reichen von der gesetzlichen Verlängerung von Feiertagen, über die Zahlung von „Quarantänegeld“ bis hin zu staatlichen Subventionen von stark betroffenen Betrieben in Ausnahmefällen. Der auf den ostasiatischen Markt spezialisierte „China Desk“ von Luther hat für Sie eine Zusammenstellung der wichtigsten Gesetze, Erlasse und Dekrete konzipiert, die Sie hier finden.

Mittelbare Auswirkungen bei Dritten (z.B. Lieferanten)

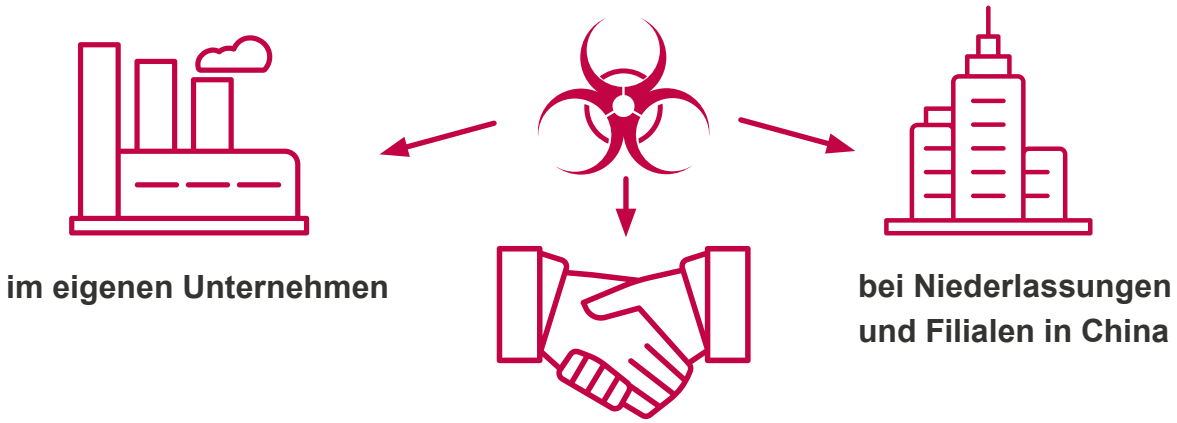
Auch die mittelbaren Gefahren durch Auswirkungen bei Dritten wie Lieferanten, Kooperations- und Absatzpartnern müssen analysiert werden. Überlegungen hinsichtlich der Konsequenzen bei Erkrankung der dortigen Belegschaft (abgesehen von einer Ansteckungsgefahr der eigenen Belegschaft) spielen hier nur eine untergeordnete Rolle, von entscheidender Bedeutung ist hier das Vertragsmanagement. Die oben aufgeführten Überlegungen zu den vertraglichen Konsequenzen müssen hier spiegelbildlich angestrengt werden, aus Sicht des eigenen Unternehmens als Gläubiger des Vertragspartners. Hinzu kommt nach Möglichkeit die Kenntnis und Übersicht über alternative Dienstleister bzw. Zulieferer, deren Kosten sich möglicherweise über den Schadensersatzanspruch statt der (ganzen/teilweisen) Leistung „wiedergeholt“ werden können.

Im Falle von Werkverträgen (z.B. Vertrag zur Programmierung von Individualsoftware, EVB-IT Systemverträge etc.) sollten die Möglichkeiten der Eigen- bzw. Ersatzvornahme evaluiert werden. Ist es dem Unternehmen praktisch möglich, kann es unter Umständen bei coronabedingten Leistungsausfällen des Vertragspartners die geschuldete Programmier-, Hardwareerstellungs- oder sonstige Leistung selber vornehmen (bzw. durch Dritte vornehmen lassen) und die hierfür entstandenen Auswirkungen vom Vertragspartner ersetzt verlangen.

Force Majeure

Standardmäßig existieren insbesondere in internationalen IT-Verträgen (vor allem Server- und Hostingverträge) Klauseln zur sog. Force Majeure („Höhere Gewalt“). Sie dienen als „Haftungsbefreiung“ von Schadensersatzpflichten im Falle von „Höherer Gewalt“. Diese Art von Klauseln führen meist ein stiefmütterliches Dasein und werden selten beachtet. Ein ausnahmsweise bestehender Anwendungsfall kann aber das Vorliegen einer Epidemie bzw. Pandemie sein.

Auswirkungen des Corona Virus



Voraussetzung für die Anwendbarkeit ist, dass das Ereignis (in China: „Änderung der objektiven Umstände“)

- nach Abschluss des Vertrages,
- aber vor dem vertraglichen Erfüllungszeitpunkt (Lieferung, Fertigstellungstermin, etc.) eingetreten ist und
- noch anhält.

Der Vertrag selbst muss also vor dem Eintritt höherer Gewalt geschlossen worden sein, sonst war das Ereignis nicht „unvorhersehbar“. Ob und wie lange sich der leistungspflichtige Vertragspartner dann wirklich auf höhere Gewalt berufen kann, ohne schadensersatzpflichtig zu werden, hängt noch von weiteren Umständen ab, z.B. ob es sich um eine Spezialanfertigung handelt oder einfache Handelsware, für die auch anderweitig Ersatz beschafft werden kann. Insbesondere im Falle von Software, selbst bei individuell angefertigter, dürfte es aufgrund der theoretisch endlos vorhandenen Grundressourcen (Know-How, Programmiersprache etc.) deutlich schwieriger sein, für das Vorliegen von Unmöglichkeit zu argumentieren als bei physischen Produkten.

Die „Haftungsbefreiung“ bezieht sich im Übrigen nur auf die Pflicht, Schadensersatz zu leisten oder eine Vertragsstrafe zu zahlen; die Pflicht zur Erfüllung der Primärschuld, z.B. Lieferung von Waren, fällt damit nicht automatisch weg. Der Schuldner kann jedoch berechtigt sein, unter Berufung auf die Grundsätze der Störung der Geschäftsgrundlage eine Vertragsanpassung zu verlangen oder die außerordentliche Kündigung zu erklären; dies hängt jedoch von den konkreten Regelungen des jeweiligen Vertrags und den Umständen des Einzelfalls ab.

Weitere rechtliche Erwägungen

Allen voranstehenden Ausführungen ist gemein, dass stets zuerst die Frage des anwendbaren Rechts (insb. deutsches gegenüber chinesischem Recht) geklärt werden muss. Regelmäßig findet sich hierzu in den Schlussbestimmungen eines Vertrages oder in den Allgemeinen Geschäfts- oder Einkaufsbedingungen ein entsprechender Passus. Gleichzeitig sollte geprüft werden, welcher Gerichtsstand im Falle eines Rechtsstreits Anwendung findet – oder ob vielleicht eine Schiedsgerichtsklausel vorhanden ist. Das Wissen um diese Frage hat konkrete Auswirkungen auf die realen Vollstreckungschancen.

Praxishinweis

So individuell wie der Krankheitsverlauf eines mit Corona infizierten Patienten ist auch das Schutz- und Maßnahmenbedürfnis von Unternehmen, die unmittelbar oder mittelbar von den Auswirkungen des Virus betroffen sind. Eine wirksame Strategie kann insofern nur bei genauer Kenntnis der Vertriebswege und Vertragswerke und der rechtlichen Rahmenbedingungen erarbeitet werden.

Weitere Informationen finden Sie auf unserer Infoseiten zu den rechtlichen Auswirkungen des Coronavirus und den arbeitsrechtlichen Implikationen aus Arbeitgebersicht.

Wir wünschen allen Lesern, dass sie vom Virus verschont bleiben.

Höchstes deutsches Datenschutzbußgeld gegen Deutsche Wohnen

Mit dem im letzten Jahr medienwirksam ergangenen Rekordbußgeld gegen die Deutsche Wohnen in Höhe von EUR 14,5 Millionen setzt sich der Trend der deutschen Datenschutzbehörden fort, mehr und höhere Bußgelder zu verhängen. Außerdem stellt der Fall anschaulich dar, welche Auswirkungen gelungene und misslungene Kooperationen mit den Datenschutzbehörden auf die Sanktionierung haben kann.

Hintergrund

Der ursprüngliche Vorwurf der Behörden gegen Deutsche Wohnen: Das Unternehmen nutze ein Archivsystems zur Erfassung personenbezogener Daten, das keine Möglichkeit zur Löschung nicht mehr erforderlicher Daten vorsah. Darin liege ein Verstoß gegen datenschutzrechtliche Verarbeitungsgrundsätze, nämlich den Grundsatz der Speicherbegrenzung und dem Grundsatz des Datenschutzes durch Technikgestaltung, wie ihn die EU-Datenschutzgrundverordnung (DSGVO) vorschreibt.

Der Bußgeldentscheid, der auf diese Verstöße folgte, fällt in einen fortlaufenden Trend der Sanktionierungsbereitschaft der deutschen Behörden. Bereits in den vergangenen Monaten zeichnete sich bei den deutschen Behörden insoweit eine größere Bereitschaft ab, den Bußgeldrahmen der DSGVO bei Datenschutzverstößen intensiver und in Gestalt höherer Bußgelder zu nutzen. Der letzte „Rekord“ lag hier bei EUR 195.000 gegen den Lieferdienst „Delivery Hero“ und selbst dieser Betrag schien im Unionsvergleich noch eher zurückhaltend. Dort arbeiteten die Behörden schon länger im Millionenbereich (UK: EUR 200 Mio. gegen British Airways; Frankreich: EUR 50 Mio. gegen Google).

Eine Gesamteinordnung der vorgenannten Bußgelder im deutschen und europäischen Vergleich finden Sie in unserem interaktiven Bußgeldatlas (hier).

Der Datenschutzverstoß: unzureichendes Löschkonzept

Die Deutsche Wohnen hätte wohl schon aufgrund der sensiblen Natur der von ihr verarbeiteten personenbezogenen Daten äußerste Sorgfalt beim Datenschutz walten lassen sollen. So verarbeitete das Unternehmen Mieter- und Interessentendaten wie beispielsweise Gehaltsnachweise, Selbstauskunftsformulare, Arbeitsverträge, sowie Steuer-, Sozial- und Krankenversicherungsdaten – teilweise speicherte sie diese Daten auch über die Beendigung der Miet- und Vertragsverhältnisse hinaus. Hierin sah die Datenschutzbehörde einen Verstoß gegen die Verarbeitungsgrundsätze der DSGVO. Demnach dürfen Unternehmen personenbezogene Daten nur so lange speichern und verarbeiten, wie dies für den Zweck, zu dem sie erhoben wurden, erforderlich ist.

Noch vor Inkrafttreten der DSGVO im Jahr 2017 rügte die Datenschutzbeauftragte im Rahmen eines ersten Prüfungstermins bereits das Vorgehen des Unternehmens. Bei einer weiteren Kontrolle im März 2019 hatte die Deutsche Wohnen trotz nachdrücklicher Aufforderung weder ihren Datenbestand

entsprechend der gesetzlichen Anforderungen bereinigt, noch konnte sie rechtliche Gründe für die fortdauernde Speicherung der Daten anführen.

Vorliegend hatte die Behörde bei der konkreten Bemessung diverse be- und entlastende Umstände zu berücksichtigen. Nachteilig wirkte sich dabei für das Immobilienunternehmen aus, dass das Archivsystem bewusst in seiner konkreten Form angelegt wurde. Entlastend wirkte sich dagegen die Bereitschaft zur Zusammenarbeit mit den Behörden und die Einleitung erster Schritte zur Behebung der Missstände aus, auch wenn diese den gesetzlichen Erfordernissen nicht genügten.

Trotz dieser fallgerechten Abwägung der Einzelumstände kam die Behörde letztlich zu der Entscheidung, dass hier ein gravierender Datenschutzverstoß vorliegt. Ein Verstoß, der bei einem sorgfältigem Ansatz zu einem Löschkonzept nicht hätte passieren müssen. Denn Lösch- und Archivierungskonzepte sind im ersten Anlauf zwar unter Umständen aufwändig, sie sind jedoch bei einem systematischen Herangehen bei weitem keine unlösbare Herausforderung. In der Regel bedarf es nur der folgenden konzeptionellen Schritte, die ein guter Datenschutzberater – gleich ob hausintern oder extern – auch ohne Weiteres mit Leben zu füllen weiß:

1. Umfangsanalyse und Bestandsaufnahme,
2. Festlegung von Löschfristen und Datenkategorien,
3. Löschverantwortlichkeit bestimmen,
4. Synergieidentifizierung und Schnittstellensuche zu anderen Compliance-Bereichen.

Praxishinweis

Mit Einführung der DSGVO hat sich der mögliche Bußgeldrahmen von vormals EUR 300.000 auf bis zu 4% des weltweiten Jahresumsatzes des Mutterkonzerns beziehungsweise bis zu EUR 20 Millionen deutlich erhöht. Im Gegensatz zu anderen EU-Staaten zögerten die deutschen Aufsichtsbehörden aber bisher bei der Ausschöpfung dieses Bußgeldrahmens. Mit der Einführung und Anwendung des neuen Bußgeldmodells dürften die Strafen in Zukunft jedoch deutlich höher ausfallen. Dadurch sollen Unternehmen weiter für Datenschutzbelange sensibilisiert, gleichzeitig aber auch ein Abschreckungseffekt erzielt werden. Das Bußgeld wird dabei zunächst schematisch anhand des Jahresumsatzes des Unternehmens ermittelt, bevor die Umstände des Einzelfalles zu einer Milderung oder Verschärfung führen können.

Digitalisierung in der Verwaltung – Die E-Rechnungsverordnung

Seit dem 27. November 2019 können Unternehmer, die im Auftrag der Bundesverwaltung tätig sind, elektronische Rechnungen einreichen. Zum November 2020 wird die elektronische Rechnungsstellung sogar verpflichtend. Unternehmer sollten die verbleibende Zeit nutzen, um sich mit den neuen Regelungen auseinanderzusetzen.

Hintergrund der Regelungen

Grundlage ist die Digitalstrategie des Bundes, mit der die Bundesregierung die Digitalisierung vorantreiben will. Insbesondere soll die Verwaltung moderner und unbürokratischer werden. Die Verordnung über die elektronische Rechnungsstellung im öffentlichen Auftragswesen des Bundes – kurz E-Rechnungsverordnung – wurde bereits am 6. September 2017 verabschiedet und regelt die Abrechnung von Leistungen nach Erfüllung öffentlicher Aufträge. Die Verordnung beruht auf einem deutschen Gesetz, das aber letztlich europäische Vorgaben umsetzen soll.

Wen betrifft die Verordnung?

Die Verordnung verpflichtet öffentliche Stellen, elektronische Rechnungen anzunehmen und weiterzuverarbeiten. Hinzu kommt künftig die Pflicht zur elektronischen Rechnungsstellung für alle im Auftrag des Bundes tätigen Unternehmer. Ausnahmen gelten lediglich für Rechnungen, die nach Erfüllung eines Direktauftrags bis zu einem Betrag von 1.000 Euro gestellt werden, bestimmte Verteidigungs- und sicherheitsspezifische Aufträge betreffen oder im Rahmen von Organleihen gestellt werden. Die E-Rechnungsverordnung gilt zunächst nur für den Bereich des Bundes. Die Bundesländer und damit auch die Kommunen werden nicht erfasst. Vielmehr müssen die Länder die europäischen Vorgaben zur E-Rechnung individuell umsetzen. Stichtag für die Behörden der Bundesländer ist hier bereits der 01.04.2020, die Pflicht für Unternehmen zur Ausstellung einer solchen E-Rechnung ist jedoch nicht einheitlich geregelt.

Welche Anforderungen werden gestellt?

Kernelement der elektronischen Rechnung ist ein strukturiertes elektronisches Format, das die automatische Verarbeitung des Dokuments ermöglicht. PDF-Dateien, Bilddokumente und eingescannte Papierrechnungen sind damit ausgeschlossen. Die Rechnung muss in dem Format ausgestellt und übermittelt werden. Für das Format sieht die Verordnung grundsätzlich den nationalen Datenaustauschstandard XRechnung vor. Hierbei handelt es sich nicht um ein eigenständiges Dateiformat, sondern um ein Datenmodell, welches im vom IT-Planungsrat als maßgeblich für die Umsetzung der europäischen Vorgaben festgelegt wurde und auf XML basiert. Dadurch wird insbesondere das von der europäischen Richtlinie geforderte Kriterium der Interoperabilität erfüllt.

Neben der grundsätzlichen Pflicht zur Nutzung der XRechnung sieht die Verordnung auch die Möglichkeit vor, eine andere Norm zu nutzen, wobei aus dieser Formulierung schon ersichtlich wird, dass XRechnung bevorzugt verwendet werden sollte. Die alternativ genutzte Norm muss den europäischen Vorgaben genügen, das heißt sie muss insbesondere auch interoperabel sein. Die europäischen Anforderungen an das Datenmodell ergeben sich aus der Definition des Europäischen Komitees für Normung CEN (Comité Européen de Normalisation). Hier bietet sich als Alternative zur XRechnung insbesondere ZUGFeRD an. Dabei handelt es sich um ein Dokumentenformat, das aus zwei Bestandteilen besteht. Es kombiniert die visuelle Darstellung der Rechnung (als PDF) und die maschinenlesbare strukturierte Darstellung der Daten (als XML). Hierdurch besteht für Unternehmen die Möglichkeit, ohne den stets erforderlichen Aufwand für die Umwandlung des nur maschinenlesbaren Formats XML, eine prüfbare und revisionssichere elektronische Rechnungslegung zu implementieren.

Die Rechnungsübermittlung muss zwingend über ein Verwaltungsportal des Bundes erfolgen, welches sich momentan allerdings noch im Aufbau befindet. Als Unternehmer muss man sich mit einem Nutzerkonto beim Verwaltungsportal registrieren, wodurch eine eindeutige und schnelle Zuordnung der elektronischen Rechnungen erfolgen soll. Zudem soll der Eingang sowie die formelle Fehlerhaftigkeit einer eingereichten E-Rechnung automatisiert erkannt und der Rechnungssteller hierüber benachrichtigt werden.

Bei der Übermittlung von Rechnungen stellt sich die Frage, welche technischen und gesetzlichen Vorgaben zu beachten sind. Insbesondere werden hier Aspekte der Datensicherheit und des Datenschutzes relevant, sofern in der E-Rechnung personenbezogene Daten enthalten sind - wovon in der Regel ausgegangen werden kann. An dieser Stelle wirkt sich die Datenschutzgrundverordnung (DSGVO) aus, die angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten fordert. Angesichts der sich stetig zuspitzenden Gefahrenlage auf dem Feld der Cybersecurity sind solche Maßnahmen unerlässlich, um die Vertraulichkeit und Integrität der Daten zu schützen und datenschutzkonform zu agieren. Beispielhaft sei hier der Mindeststandard der Transportverschlüsselung genannt, der aber bei kritischen Daten sogar um eine Ende-zu-Ende-Verschlüsselung ergänzt werden sollte.

Unser Kommentar

Mit Verabschiedung der E-Rechnungsverordnung verfolgt die Bundesregierung ihre Digitalstrategie weiter. Mit der Einführung der Pflicht zur elektronischen Rechnungsstellung geht die Bundesregierung über die von der europäischen Richtlinie geforderten Maßnahmen hinaus, die lediglich eine Pflicht der Verwaltung zur Entgegennahme von elektronischen Rechnungen vorgibt. Gleichwohl kann die Verpflichtung zur E-Rechnung die Entwicklung eines einheitlichen Standards in den Unternehmen fördern und so auch die elektronische Rechnungsstellung von Unternehmern untereinander vereinfachen.

Dies könnte neben den offensichtlichen Kosteneinsparungen bei der Rechnungsstellung auch die Optimierung von Unternehmensprozessen mit sich bringen und so positive Effekte für die Wirtschaft erzielen. Bei der Umsetzung der E-Rechnungsverordnung sollten Unternehmen aber auch die gesetzlichen Vorgaben zum Datenschutz sowie zur IT-Sicherheit stets im Blick haben. Anderenfalls drohen nicht nur öffentlichkeitswirksame Datenpannen, sondern gegebenenfalls auch Bußgelder und Schadensersatzansprüche.

Das Cookie-Urteil des EuGH – Offene Fragen rund um den Praxis-Einsatz von Cookies

Auch nach der jüngsten europäischen Rechtsprechung zum Einsatz von Cookie-basierten Diensten auf Webseiten verbleiben rechtliche Fragezeichen im Hinblick darauf, welche Anforderungen an die Gestaltung eines rechtskonformen Consent-Mechanismus zu stellen sind.

Nachtrag zu EuGH, Urt. v. 01. Oktober 2019, Az. C-673/17

In der Praxis sehen sich Website-Betreiber mit der Frage konfrontiert, wie sie das nunmehr von dem Europäischen Gerichtshof (EuGH) vertretene Einwilligungserfordernis mit einer möglichst hohen Conversion-Rate betreffend den Einsatz von Cookie-basierten Marketingtools vereinbaren können. Dabei verbleibt nach der Entscheidung des EuGH ein erheblicher Spielraum, der die Website-Betreiber vor neue rechtliche und kommerzielle Herausforderungen stellt.

Hintergrund

Der EuGH hat mit Urteil vom 1. Oktober 2019 (Az. C-673/17) entschieden, dass der Einsatz von Cookies, die nicht zwingend für den Betrieb einer Webseite erforderlich sind, ein sog. „Opt-In" erfordert, d.h. eine aktive und informierte Einwilligung jedes betroffenen Besuchers (siehe dazu unsere ausführliche Urteilsbesprechung).

Mit seiner richtungsweisenden Entscheidung hat der EuGH zwar einen wesentlichen Beitrag zur Beseitigung von Rechtsunsicherheiten im Zusammenhang mit dem seit langem heftig umstrittenen Einsatz von Cookies und darauf beruhenden Marketingtools geleistet. Jedoch bleiben indes viele Einzelfragen im Hinblick auf die konkrete Gestaltung eines Consent-Managements, das den gesetzlichen Vorgaben genügt, weitestgehend unbeantwortet.

Unser Kommentar

Bei der Bewertung des Urteils ist zu beachten, dass dieses sich nicht direkt mit den Anforderungen befasst, die an ein Cookie-Banner oder einen ähnlichen Consent-Mechanismus zu stellen sind. Vielmehr bewertet der EuGH unmittelbar lediglich den spezifischen Fall, in dem die Einwilligung in den Einsatz eines Analysecookies gemeinsam mit einer übergeordneten Erklärung, nämlich der Anmeldung zu einem Gewinnspiel, durch ein vorangekreuztes Kästchen und mithin „en passant", d.h. beiläufig, erfolgt.

Offen bleiben somit diverse Rechtsfragen im Zusammenhang mit der Gestaltung eines „aktiven" und „informierten" Consent-Mechanismus, der bei Aufruf einer Seite ausschließlich die Einwilligung in den Einsatz von Cookies und keine sonstigen Erklärungen behandelt. Die konkrete Gestaltung eines Cookie-Banners kann indes für die Bereitschaft der Nutzer, ihre Einwilligung in den Einsatz von Trackingtools zu erteilen oder zu verweigern, von grundlegender Bedeutung sein.

Nicht entschieden hat der EuGH beispielsweise,

- ob es Website-Betreibern gestattet ist, den Nutzern eine pauschale Einwilligung in den Einsatz sämtlicher Cookies zu ermöglichen,
- ob die Nutzung der Website von einer Erteilung einer Einwilligung in den Einsatz gewisser Cookies abhängig gemacht werden kann (sog. Kopplung),

- ob Gestaltungen, die den nur flüchtig agierenden Besucher intuitiv zu einer Einwilligung verleiten sollen (bspw. grafische Hervorhebung eines Buttons „Sämtliche Cookies akzeptieren“) rechtmäßig sind (sog. „Nudging“ bzw. „Dark Pattern“),
- ob es ausreichend ist, eine Ablehnung von Cookies ausschließlich über Cookie-Detaileinstellungen zu ermöglichen,
- ob vorangekreuzte Kästchen im Rahmen von Cookie-Detaileinstellungen rechtmäßig sind,
- welche konkreten Kriterien zur Bestimmung eines sog. „erforderlichen Cookies“, das auch ohne ausdrücklich Einwilligung des Nutzers zum Einsatz kommen kann, heranzuziehen sind,
- ob neben dem Erfordernis einer Einwilligung gemäß der sog. ePrivacy-Richtlinie auch eine datenschutzrechtliche Einwilligung gemäß der DSGVO erforderlich und damit im Falle eines Verstoßes der erhebliche Bußgeldrahmen der DSGVO eröffnet ist.

Die Datenschutzaufsichtsbehörden vertreten in diesen Punkten in der Regel eher restriktive Ansichten. So lehnen sie bisher unter anderem die Kopplung der Nutzung einer Website (oder von anderen Diensten) mit der Erteilung einer Einwilligung sowie vorangekreuzte Kästchen grundsätzlich ab. Auch sind die Aufsichtsbehörden der Meinung, dass es bei Cookies stets einer datenschutzrechtlichen Einwilligung nach der DSGVO bedarf.

Die deutsche Rechtsprechung weicht jedoch teilweise von den Ansichten der Aufsichtsbehörden ab: so hat das OLG Frankfurt (Urt. v. 27.06.2019, Az. 6 U 6/19) entschieden, dass eine Kopplung erlaubt sei. Der Tausch von „Daten gegen Leistung“ sei demnach zulässig, sofern der Einwilligende nur ausreichend und transparent über die Datenverarbeitungen informiert werde.

Dies zeigt, dass es sich lohnen kann, gegen Entscheidungen der Aufsichtsbehörden gerichtlich vorzugehen. Um langwierige und gegebenenfalls kostspielige Auseinandersetzungen mit den Behörden zu vermeiden, ist jedoch stets eine genaue datenschutzrechtliche Prüfung der eingesetzten Cookies zu empfehlen. Website-Betreiber sollten dabei im Rahmen der konkreten Gestaltung des Einwilligungs-Mechanismus die bestehenden Risiken und Spielräume beachten, um eine rechtlich vertretbare und gleichzeitig kommerziell möglichst vorteilhafte Lösung umzusetzen.

Online-Händlern droht Haftung wegen Markenrechtsverletzungen Dritter

Für Online-Händler, die auch den Verkauf von Produkten durch Drittanbieter zulassen (z. B. der sog. Marketplace bei Amazon), könnte es schon bald sehr unangenehm werden. In einem Verfahren gegen Amazon vor dem Europäischen Gerichtshof (EuGH, Az. C-567/18) soll nach Ansicht des Generalanwalts der Versandriese künftig verstärkt für Markenrechtsverletzungen Dritter auf seinem Marketplace zur Verantwortung gezogen werden. Folgt der EuGH der Auffassung des Generalanwalts, könnte dies zu einer grundlegenden Veränderung im gesamten Onlinehandel mit Drittanbietern führen.

Hintergrund

Hintergrund des Gutachtens des Generalanwalts ist ein Rechtsstreit in Deutschland zwischen dem Parfum- und Kosmetikkonzern Coty Germany und der Online-Handelsplattform Amazon. Im Rahmen von Testkäufen hatte Coty festgestellt, dass Drittanbieter über den Amazon-Marketplace das Parfum „Davidoff Hot Water“ verkauften. Coty hält die Lizenz an der Marke „Davidoff“ und hatte dem Verkauf des Parfums zuvor nicht zugestimmt. Coty hatte daraufhin die Drittanbieter sowie Amazon auf Unterlassung und Schadensersatz verklagt. Das Angebot selbst war Teil des Programms „Versand durch Amazon“, welches Drittanbietern ermöglicht, ihre Waren in Amazon-Logistikzentren zu lagern. Diese werden dann im Anschluss an eine Bestellung durch Amazon verpackt und an den Kunden versendet. Der Kaufvertrag kommt hierbei nicht zwischen dem Kunden und Amazon, sondern zwischen dem Kunden und dem Drittanbieter zustande. Nach Auffassung des Parfumkonzerns ist Amazon durch das Lagern und Verpacken der Ware für etwaige Markenrechtsverletzungen des Drittanbieters zumindest mitverantwortlich.

Eine Inanspruchnahme des Versandkonzerns blieb jedoch bislang ohne Erfolg. Sowohl das Landgericht als auch Oberlandesgericht München ließen ein bloßes Verwahren oder Versenden markenrechtsverletzender Waren für einen Dritten, der die Waren vertreibt, für eine Inanspruchnahme nicht ausreichen. Der Bundesgerichtshof (BGH) setzte schließlich das Verfahren aus und suchte Rat beim EuGH.

Vorlagefrage des BGH und Gutachten des Generalanwalts des EuGH

Der BGH hatte dem EuGH Fragen zur Auslegung des Art. 9 der Unionsmarken-Verordnung ((EU) 2017/1001) vorgelegt. Konkret sollte der EuGH klären, ob Personen bzw. Unternehmen, die für einen Dritten markenrechtsverletzende Waren lagern, ohne vom Rechtsverstoß Kenntnis zu haben, die Ware im Sinne der Verordnung „besitzen“, wenn nicht die Person bzw. das Unternehmen selbst, sondern allein der Dritte beabsichtigt, die Ware anzubieten oder in Verkehr zu bringen.

Amazon beruft sich darauf, dass das bloße Verwahren oder Versenden von Waren für einen Dritten regelmäßig nicht zu dem Zwecke erfolge, die Waren selbst anzubieten oder in Verkehr zu bringen. Eine verbotene Benutzungshandlung setze einen solchen qualifizierten Zweck jedoch voraus. Eine Haftung sei damit in der vorliegenden Konstellation ausgeschlossen.

Aus Sicht des Generalanwalts am EuGH, Manuel Campos Sánchez-Bordona, soll Amazon unter Umständen jedoch für Markenrechtsverletzungen auf dem Amazon-Marketplace haften. Dies geht aus seinen Schlussanträgen hervor, die am 28. November 2019 veröffentlicht wurden (Rechtssache C-567/18). Reine Lagerhalter, die lediglich Hilfsaufgaben übernehmen, seien von der Haftung befreit, nicht jedoch solche Unternehmen, die sich aktiv am Vertrieb der Ware beteiligen. Bei Amazon betreffe dies solche Waren, die im Rahmen des Programms „Versand durch Amazon“ vertrieben werden. In diesem Zusammenhang trete Amazon nicht als neutraler Lagerhalter auf, sondern beteilige sich aktiv am Vertrieb der Waren und lagere die Waren zum Zweck des Anbietens und Inverkehrbringens. Auch die fehlende Kenntnis von Markenrechtsverletzungen führe nicht zur Haftungsbefreiung des Versandkonzerns. Aufgrund der „wesentlichen Beteiligung am Vertrieb“ werde das Unternehmen stets aufgefordert, besonders sorgfältig die Rechtmäßigkeit der dort gehandelten Waren zu überprüfen. Nach Ansicht des Generalanwalts sollten sich Betreiber von Onlineplattformen bewusst sein, dass

sie ohne Kontrolle der Waren als Vertriebskanal für illegale, gefälschte, gestohlene oder unethische Produkte dienen können. Damit distanziert sich der Generalanwalt des EuGH deutlich von der bisherigen Rechtsprechung der nationalen Gerichte.

Es bleibt abzuwarten, welcher Auffassung sich der EuGH in dieser Sache anschließt. Sein Grundsatzurteil, auf dessen Basis sodann der BGH den Einzelfall entscheiden wird, wird innerhalb der nächsten Monate erwartet.

Unser Kommentar

Folgt der EuGH, wie so häufig, der Ansicht des Generalanwalts, könnte dies zu grundlegenden Veränderungen im Onlinehandel führen, die sich nicht nur auf Amazon, sondern auch auf ähnlich agierende Unternehmen wie z.B. Ebay auswirken könnten.

Für Amazon stellt das Programm „Versand durch Amazon“ bislang einen wesentlichen Teil des Geschäftsmodells dar, da es nicht nur Amazon selbst, sondern auch den Verbrauchern Vorteile bringt und zusätzlich die Umwelt schont. Das Programm ermöglicht beispielsweise, dass bei der Bestellung mehrerer Teile durch den Kunden die Ware in nur einer Paketsendung verschickt werden kann. Obgleich eine verschärfte Haftung der Onlineplattformen verhindern würde, dass sich Onlinehändler, die sich an einem Verkaufsprozess beteiligen, aus der Verantwortung ziehen können, könnten die erhöhten Haftungsrisiken im Ergebnis dazu führen, dass derartige Leistungen zukünftig nicht mehr angeboten werden. Um das Haftungsrisiko so gering wie möglich zu halten, wären Handelsplattformen, die Produkte von Drittanbietern vertreiben, dazu angehalten, die gehandelten Produkte regelmäßig und fortlaufend auf ihre Legalität hin zu überprüfen. Die betroffenen Unternehmen kämen insofern nicht umhin, weniger zusätzliche Leistungen (wie die Übernahme des Versands) anzubieten oder mehr Mittel zur Verfolgung von Markenrechtsverletzungen aufzuwenden, um höhere Schadensersatzzahlungen zu vermeiden.

Einen positiven Effekt verspricht das Gutachten des Generalanwalts allerdings für die Inhaber der verletzen Marken: etwaige Ansprüche könnten dann nicht mehr nur gegenüber dem Händler, sondern auch gegenüber Amazon durchgesetzt werden. In Anbetracht der Schwierigkeiten bei der Rechtsdurchsetzung gegen ausländische Händler, dürfte dies eine ganz erhebliche Erleichterung in der Verteidigung der eigenen Marken bedeuten. Die Entscheidung des EuGH ist daher mit Spannung zu erwarten.

Influencer-Marketing: Werbekennzeichnung auf Instagram

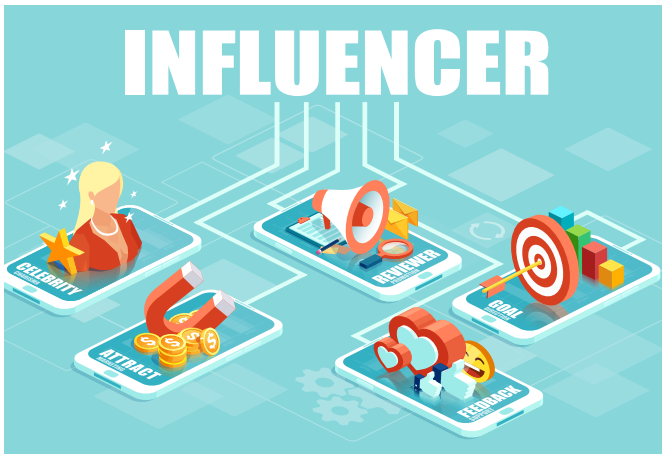
Mit seinem Beschluss vom 24. Oktober 2019 hat nunmehr auch das Oberlandesgericht Frankfurt am Main entschieden, dass Influencer Verlinkungen auf Instagram zu dem Account des jeweiligen Herstellers eines präsentierten Produkts als Werbung kennzeichnen müssen, da die Waren und/oder Dienstleistungen im geschäftlichen Verkehr präsentiert werden. Ein Unterlassen der Kennzeichnung stelle ein wettbewerbswidriges Verhalten dar, unabhängig davon ob für die Verlinkung eine Gegenleistung erbracht bzw. erwartet wurde oder nicht.

OLG Frankfurt a.M., Beschl. v.24.10.2019, Az. 6 W 68/19

Hintergrund

Im Rahmen eines einstweiligen Verfügungsverfahrens ist ein Verlag gegen eine Influencerin vorgegangen, die auf ihrem personalisierten Instagram-Account regelmäßig Fotos von sich mit diversen Produkten und Dienstleistungen veröffentlicht hat. Die abgebildeten Produkte bzw. Dienstleistungen wurden teilweise mit den Instagram-Accounts der Anbieter verlinkt, ohne den jeweiligen Post jedoch als Werbung oder Anzeige zu kennzeichnen. In zumindest zwei ihrer Begleittexte, die jeweils unterhalb des Beitrags zu erkennen waren, bedankte sie sich zudem bei verlinkten Anbietern für die Einladung zu Reisen.

Der Verlag argumentierte, dass diese Produktpräsentation eine verbotene redaktionelle Werbung darstelle und deshalb unlauter sei. Aus diesem Grund hat er im Wege eines einstweiligen Verfügungsverfahrens rechtliche Schritte gegen die Influencerin eingeleitet und beim erstinstanzlich zuständigen Landgericht Frankfurt am Main die Unterlassung des wettbewerbswidrigen Verhaltens beantragt – jedoch ohne Erfolg.



Das Landgericht Frankfurt verneinte das Vorliegen einer wettbewerbsrechtlich relevanten Irreführung durch die Influencerin. Die Art der Posts war nach Ansicht der Kammer nicht dazu geeignet, die Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, da eine Verlinkung lediglich auf die Instagram-Seiten der Anbieter erfolge und eben gerade nicht auf die entsprechenden Shop-Seiten. Darüber hinaus liege keine kommerzielle Kommunikation vor, da die Angaben unabhängig und ohne finanzielle Gegenleistung erfolgt seien.

Der Verlag hat gegen diesen Beschluss sodann erfolgreich Beschwerde eingelegt.

Die Entscheidung

Entgegen der Auffassung der Kammer des Landgerichts Frankfurt handelte die Influencerin nach Ansicht des zuständigen Senats des Oberlandesgerichts Frankfurt unlauter im Sinne des Gesetzes gegen unlauteren Wettbewerb (UWG). Ihr Instagram-Account stelle eine geschäftliche Handlung dar, wobei die Posts den Absatz der präsentierten Produkte steigern und das Image des beworbenen Herstellers fördern solle. Der kommerzielle Zweck des Posts habe sich dabei jedoch weder unmittelbar aus den Umständen, noch aus einer Kennzeichnung ergeben. Da die Influencerin als Privatperson auftrete, die andere an ihrem Leben teilhaben lässt, sei sie gerade keine Werbefigur, sondern eben eine Influencerin.

Der Senat hat den Account insgesamt als kommerziell eingeordnet, da nicht entscheidend sei, ob für den einzelnen Post eine Gegenleistung erbracht bzw. erwartet werde. So nutze die Influencerin – die gleichzeitig Autorin eines Spiegelbeststellers ist – ihre eigene Bekanntheit auf Instagram aus, um auch ihre eigenen Produkte und sich selbst zu vermarkten und hierdurch Einkünfte zu erzielen.

Durch die Art und Weise der Posts sei es – nach Auffassung des Senats – für den privaten Nutzer nicht ohne weiteres erkennbar, ob es sich bei dem Beitrag um eine Werbemaßnahme oder aber eine private Meinungsäußerung der Influencerin handele. Deshalb seien die Posts geeignet, den Verbraucher zu einer geschäftlichen Handlung zu veranlassen, die er andernfalls nicht getroffen hätte. Entscheidend sei nämlich, dass die Follower zum Anklicken der markierten Unternehmen motiviert werden. Der Beschluss des Oberlandesgerichts Frankfurt ist nicht anfechtbar.

Unser Kommentar

Die zunehmende Verlagerung der Tätigkeit der Influencer vom privaten in den geschäftlichen Bereich bedingt Pflichten, die es beim Posten und Verlinken bestimmter Inhalte in den sozialen Medien zu beachten gilt. In diesem Zusammenhang führten die sog. Kennzeichnungspflichten in der Vergangenheit immer wieder zu rechtlichen Problemen und Unklarheiten. Da bislang noch keine höchstrichterliche Rechtsprechung zu der Frage existiert, wann Influencer-Marketing kennzeichnungspflichtige Werbung und wann eine bloße Meinungsäußerung darstellt, muss zur rechtlichen Klärung aller auftretender Fragen auf die oft uneinheitliche Rechtsprechungslinie der Instanzgerichte abgestellt werden.

Die nunmehr erlassene Entscheidung des Oberlandesgerichts Frankfurt zeigt dabei einmal mehr, dass Influencer bei ihrem Social-Media-Auftritt streng auf eine Werbekennzeichnung von Posts achten sollten, um gerichtliche Verfahren zu vermeiden. Die Tatsache, dass Influencer über ihren Social-Media-Account neben privaten auch werbliche Einträge veröffentlichen, ist für den Betrachter bzw. Verbraucher nicht in jedem Fall erkennbar. Ziel der Rechtsprechung des Oberlandesgerichts Frankfurt am Main ist es, den Schutz des Verbrauchers vor versteckter Werbung zu gewährleisten und ihm eine informierte Kaufentscheidung zu ermöglichen. Nur wenn der Verbraucher weiß, ob es sich bei der Produktempfehlung um eine private Meinung oder eine Werbung handelt, kann dieser eine entsprechende Kaufentscheidung treffen.

Da sich die rechtliche Situation zu dieser Thematik noch sehr uneinheitlich darstellt, sollte in jedem Fall vor der Veröffentlichung eines Posts, in dem eine Ware und/oder eine Dienstleistung gekennzeichnet wird, überprüft werden, ob dieser bereits als sog. Influencer-Marketing eingestuft werden könnte.

Mehr zu dem Thema erfahren Sie auf unserer Übersichtsseite zum Influencer-Marketing und Recht.

Schrems gegen Facebook – Bleiben Standard-datenschutzklauseln weiterhin zulässig?

Am 19. Dezember 2019 wurden die Schlussanträge des Generalanwalts im Schrems II Verfahren veröffentlicht, das sich mit dem Datentransfer nach der DSGVO in Länder außerhalb der EU beschäftigt. Der Generalanwalt spricht sich für die Wirksamkeit der Standardvertragsklauseln aus, äußert sich aber auch kritisch in Bezug auf den Privacy Shield. Schrems selbst bezeichnet die Stellungnahme des Generalanwalts als eine „schallende Ohrfeige" für die irische Datenschutzbehörde und für Facebook.

Hintergrund

Der österreichische Datenschützer Maximilian Schrems und Facebook streiten sich seit Jahren vor Gericht. Der Rechtsstreit wird nun zum zweiten Mal vor dem EuGH verhandelt. Mit den Schlussanträgen des Generalanwalts ist die mündliche Phase des Verfahrens abgeschlossen. Die Schlussanträge enthalten eine rechtliche Analyse der für den Rechtsstreit entscheidenden Fragen und enden mit einem Entscheidungsvorschlag. Diesem muss der EuGH nicht folgen; gleichwohl können die Schlussanträge häufig aufzeigen, in welche Richtung der Gerichtshof entscheiden wird.

Nach der Europäischen Grundrechtecharta hat jede Person das Recht auf Achtung ihres Privatlebens und auf den Schutz der sie betreffenden personenbezogenen Daten. Außerdem muss ein wirksamer Rechtsbehelf zur Verfügung stehen, mit dem eine Rechtsverletzung gerichtlich überprüft werden kann. Die Verletzung ebendieser Rechte durch die Datenübertragung in die USA unter Nutzung sog. Standarddatenschutzklauseln (Standard Contract Clauses, SCC) steht gerade auf dem Prüfstand.

SCC sind ein Instrument der Datenschutzgrundverordnung (DSGVO), die eine datenschutzkonforme Datenübermittlung in Länder außerhalb der EU und des EWR ermöglichen. Es handelt sich dabei um vorformulierte Vertragsklauseln, die zwischen dem Verantwortlichen in der EU (dem Datenexporteur) und dem Datenempfänger im Drittland vereinbart werden. Sie verpflichten den Datenempfänger auf die Einhaltung des Datenschutzes und sollen so ein angemessenes Datenschutzniveau gewährleisten. Die Europäische Kommission hat drei Zusammenstellungen von SCC erarbeitet. In der Praxis sind diese ein gängiges Mittel im internationalen Datenverkehr.

Die Vorlagefragen

Der irische High Court hat dem EuGH eine Reihe von Fragen vorgelegt, mit denen er im Wesentlichen die Wirksamkeit der SCC in Frage stellt. Ausgangspunkt ist die Feststellung der gezielten und massenhaften Überwachung durch die amerikanischen Regierungsbehörden unter gleichzeitigem Mangel von Rechtsbehelfen für EU-Bürger. Angesichts dieser Feststellungen könnte nach Ansicht des irischen Gerichts eine Verletzung der Europäischen Grundrechte (Recht auf Achtung des Privatlebens, Schutz personenbezogener Daten, Recht auf einen wirksamen Rechtsbehelf) durch die Übertragung von Daten auf Grundlage der SCC in die USA in Betracht kommen. Die SCC gelten nur zwischen dem Datenexporteur und dem Datenimporteur und entfalten gegenüber nationalen Behörden eines Drittlandes keine Bindungswirkung. Dies könnte in Verbindung mit den weitreichenden Befugnissen zum Datenzugriff der amerikanischen Behörden dazu führen, dass die SCC keine geeigneten Garantien für den Schutz der personenbezogenen Daten bieten können. Konsequenz hieraus sei letztlich die Unwirksamkeit der SCC.

Die Schlussanträge

In seinen Schlussanträgen sieht der Generalanwalt keinen Anlass, von der Unwirksamkeit der SCC auszugehen. Als Ausgangspunkt seiner Überlegungen stellt er fest, dass die Wirksamkeit der SCC von dem Datenschutzniveau des Drittlands unabhängig sei. Die SCC sollen nämlich gerade eventuelle Unzulänglichkeiten im Vergleich mit dem europäischen Datenschutzniveau ausgleichen, indem sie geeignete Garantien für den Schutz personenbezogener Daten bieten. Die Tatsache, dass die Sicherheitsbehörden in den USA weitreichenden Zugriff auf personenbezogene Daten haben, könne die Wirksamkeit der SCC daher nicht generell in Frage stellen.

Nach Ansicht des Generalanwalts hängt die Wirksamkeit der SCC vielmehr davon ab, ob diese die Möglichkeit vorsehen, einzelne Datenübertragungen auszusetzen oder zu verbieten. Es könne nämlich sein, dass die Rechtsordnung eines Drittlandes dem Datenempfänger Pflichten auferlegt, die es ihm unmöglich machen, seine in den SCC geregelten Pflichten zu erfüllen. Bei einer Verletzung der SCC müssten diese aber Mechanismen vorsehen, die Datenübertragung auf ihrer Grundlage zu unterbinden. Dies ist nach Ansicht des Generalanwalts der Fall.

Die von der Kommission beschlossenen SCC enthalten Klauseln, wonach der Verantwortliche oder – falls dieser nicht handelt – die Aufsichtsbehörden die Datenübermittlung aussetzen oder verbieten können. Hierbei haben diese nach Ansicht des Generalanwalts nicht nur das Recht, sondern auch die Pflicht, entsprechende Maßnahmen zu ergreifen, wenn sich nach einer Prüfung des Einzelfalls ergibt, dass die Rechtsordnung des Drittlandes der Anwendung der SCC widerspricht und damit einem angemessenen Schutz für die übermittelten Daten entgegensteht. Bei einem Konflikt zwischen den durch die SCC auferlegten datenschutzrechtlichen Pflichten und den Bestimmungen einer ausländischen nationalen Rechtsordnung sollen der Verantwortliche oder die Aufsichtsbehörde die Datenübermittlung aussetzen oder verbieten.

Die Wirksamkeit des Privacy Shield

Obgleich es nach Ansicht des Generalanwalts im vorliegenden Fall nicht darauf ankam, hält er es trotzdem für angebracht, einige Ausführungen zum Privacy Shield zu machen. Dieses wurde vom High Court in seinen Vorlagefragen zumindest teilweise einbezogen. Beim Privacy Shield handelt es sich um einen Beschluss der Kommission, auf deren Grundlage Daten in die USA übertragen werden können. Der Nachfolger des Safe Harbor Abkommens steht unter Datenschützern aus den gleichen Gründen, die schon zu dessen Aufhebung geführt hatten, massiv in der Kritik. So steht auch der Generalanwalt dem Privacy Shield kritisch gegenüber.

Ausgangspunkt der Überlegungen zum Privacy Shield sind die durch Edward Snowden aufgedeckten Überwachungsmaßnahmen der US-Behörden. Sie begründen Zweifel an dem Bestehen eines der DSGVO im wesentlichen vergleichbaren Schutzniveau für den Schutz personenbezogener Daten. Gerade dies war aber Grundlage des Beschlusses zum Privacy Shield. Die Rechtsgrundlage für die Überwachungsmaßnahmen im amerikanischen Recht sind nach Ansicht des Generalanwalts nicht klar und präzise genug formuliert, um Rechtssicherheit zu bieten und um Missbrauch vorzubeugen. Zwar könne der Schutz der nationalen Sicherheit eine Einschränkung des durch DSGVO garantierten Datenschutzes rechtfertigen. Diese müssten aber mit Schutzmaßnahmen einhergehen, die im Wesentlichen dem von der DSGVO geforderten Schutzniveau entsprechen.

Insofern ist problematisch, dass die Maßnahmen der US-Behörden weder im Vorfeld noch im Nachhinein von einer unabhängigen Stelle überprüft werden. Eine Benachrichtigung der betroffenen Person erfolgt nicht und ein wirksamer Rechtsbehelf gegen die Maßnahmen ist nicht vorgesehen. Auch die im Privacy Shield vorgesehene Einrichtung einer Ombudsperson ändert diese Einschätzung nicht.

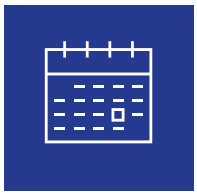
Unser Kommentar

Die Stellungnahme des Generalanwalts nimmt die Verantwortlichen und die Aufsichtsbehörden in die Pflicht. Diese müssen auch bei Verwendung der Standardvertragsklauseln weiter überprüfen, ob die Datenübermittlung in einen Drittstaat DSGVO-konform ist und anderenfalls die Datenübermittlung unterbinden. Im Verlauf des Verfahrens hatten viele Datenschützer befürchtet, der EuGH werde die Standardvertragsklauseln für unwirksam erklären. Dies hätte weitreichende Folgen für den internationalen Datenverkehr. Sollte der EuGH den Schlussanträgen folgen, kann diesbezüglich erst einmal Entwarnung gegeben werden. Sicher ist das jedoch nicht; Beobachter des Verfahrens stellten fest, dass die Fragen des Gerichts deutlich kritischer ausfielen als die Schlussanträge des Generalanwalts.

Die Stellungnahme zum Privacy Shield wird sich zwar voraussichtlich nicht auf den Ausgang dieses konkreten Verfahrens auswirken; gleichwohl kann sie Einfluss auf die Rechtsprechung des EuGH in einem anderen Verfahren haben. Mitte Januar 2020 werden die Schlussanträge in einem Verfahren erwartet, in dem die Wirksamkeit des Privacy Shields überprüft wird. Hier stehen sich die Organisation La Quadrature du Net und die Europäische Kommission gegenüber, die von diversen Staaten und Unternehmen unterstützt wird.

Es bleibt daher abzuwarten, ob der EuGH internationale Transfers mit seinen Entscheidungen erheblich erschwert oder gar vollständig verhindert. Vorzugswürdiger wäre jedoch ein Mittelweg, der zumindest eine der Transfermöglichkeiten zulässt, um den Bedürfnissen einer globalisierten Wirtschaft – insbesondere im Bereich der IT und Datenverarbeitung – ausreichend Rechnung zu tragen.

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: MR.Cole_Photographer/Getty Images: Seite 1; da-kuk/iStockphoto: Seite 3; AA+W/Adobe Stock: Seite 6; peterschreiber.media/Adobe Stock: Seite 8; Monster Ztudio/Adobe Stock: Seite 9; Tevarak/iStockphoto: 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, 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

JUVE 2019 AWARDS
Kanzlei des Jahres

Rechts- und Steuerberatung | www.luther-lawfirm.com