LOSCHELDER

Newsletter Datenschutzrecht
Mai 2021

Sehr geehrte Damen und Herren,

Datenschutz und Corona: Einen weiteren Höhepunkt dieser explosiven Mischung erleben wir aktuell. So arbeiten die Behörden mit den dazu beauftragten Unternehmen momentan an einem digitalen Impfnachweis, der den gelben Impfpass ergänzen soll. Impflinge sollen auf diese Weise mittels Smartphone eine vollständige Impfung nachweisen können. Für Diskussion sorgt dabei der Umstand, dass zum Zeitpunkt der Einführung der App bereits Geimpfte einen QR-Code per Post erhalten sollen, den sie in der App einscannen können, um die Bestätigung durchzuführen. Denn die Postadresse liegt nicht überall vor und wurde, wenn, regelmäßig zu anderen Zwecken erhoben – einmal mehr ist die Umsetzung der Digitalisierung holprig, späte Umsetzungserwägungen erschweren die sichere datenschutzkonforme Umsetzung.

Wir haben Ihnen zudem weitere spannende Einblicke mitgebracht: In unserem ersten Beitrag stellen wir Ihnen den Verordnungsentwurf der EU-Kommission zur KI-Regulierung vor – ein knapper Überblick, der einen Einblick in die möglicherweise bevorstehende Revolution gibt. Im zweiten Beitrag erläutern wir Ihnen, wie es um die langerwartete ePrivacy-Verordnung steht und welche Regelungen derzeit für den Cookie-Einsatz zu erwarten sind – auch hier steht hoffentlich eine Lösung des schon so lange währenden Prozesses an. Sodann betrachten wir aktuelle Fälle, die die Risiken im Umgang mit sozialen Medien und das Erfordernis datenschutzrechtlicher Regulierung einmal mehr in den Mittelpunkt des öffentlichen Interesses stellen. Den „Schrems II"-Hilferuf der deutschen Wirtschaft verarbeiten wir schließlich in Beitrag 4. Zu guter Letzt stellen wir Ihnen interessante Bußgeldverfahren sowie bemerkenswerte gerichtliche und behördliche Entscheidungen vor.

Auch würden wir uns freuen, Sie zu unserem nächsten Lunch@Loschelder-Webinar zur **Rollenverteilung im Datenschutzrecht am 16.06.2021 um 12.00 Uhr** begrüßen zu dürfen. Weitere Informationen dazu finden Sie unter https://loschelder.de/de/webinare.html, melden Sie sich gerne (kostenfrei) an unter webinare@loschelder.de.

Inhalt

Kommissionsvorschlag einer Künstliche-Intelligenz-Verordnung

Künstliche Intelligenz (KI) als Technik der Zukunft – und diese Zukunft möchte die Europäische Union mitgestalten. Deshalb hat die Europäische Kommission Mitte April ihren Vorschlag für eine Künstliche-Intelligenz-Verordnung veröffentlicht. Der Vorschlag beinhaltet erhebliches Potential, auch hinsichtlich der Mitgestaltung dieser Zukunft aus der EU heraus. Grund genug, schon in diesem frühen Stadium einen Überblick zu wagen.

In Sachen digitaler Regulierung ist der Europäischen Kommission momentan keine Untätigkeit vorzuwerfen. Nachdem Sie im November letzten Jahres Vorschläge für einen Digitalen-Dienste-Rechtsakt und einen Data-Governance-Rechtsakt veröffentlichte (wir berichteten dazu in unserem Newsletter aus Januar), folgt nun der Entwurf eines weiteren, langerwarteten Regulierungsprojekts: Mitte April stellte die Kommission ihren Vorschlag für die Regulierung von KI vor, die Künstliche-Intelligenz-Verordnung (Artificial Intelligence Act, englischer Volltext sowie deutsche Pressemitteilung). Ein weiterer Schritt, um die EU und den Binnenmarkt in digitaler Hinsicht zukunftsfest zu machen.

Für die KI-Verordnung hatte die Kommission schon im Februar 2020 ein Weißbuch zur Künstlichen Intelligenz veröffentlich, das von einer über 50-köpfigen Expertenkommission erstellt wurde und nun die wesentliche Grundlage für den Verordnungsvorschlag bildet.

Rechtsgüterschutz und Entwicklungsoffenheit – Der risikobasierte Ansatz

Ziel der EU-Kommission ist es, mit der KI-Verordnung ein Rahmenwerk zu schaffen, das einerseits offen genug ist, um die Entwicklung und Nutzung künstlicher Intelligenz nicht zu blockieren, andererseits aber den Gefahren und Risiken für wesentliche Rechtsgüter und Grundrechte gerecht wird. Deshalb wird – wie auch schon in der DSGVO – ein risikobasierter Regulierungsansatz gewählt. Im Entwurf zeigt sich das in der Einteilung von KI in verschiedene Risikoklassen:

- KI mit **unannehmbarem Risiko**: Dies ist KI, die die Rechte, die Lebensgrundlage oder die Sicherheit von Personen beeinträchtigt und deren Einsatz wegen des unannehmbaren Risikos für diese wichtigen Rechtsgüter verboten werden

soll. Hierzu zählt KI, die den freien Willen der Nutzer durch „unterschwellige“ oder „ausnutzende Praktiken“ manipuliert. In ihrer Pressemitteilung nennt die EU-Kommission das Beispiel von KI-Software in sprachgesteuerten Spielzeugen, die Minderjährige zu gefährlichem Verhalten animieren.

- KI mit **hohem Risiko**: Ob von einer KI ein hohes Risiko ausgeht, richtet sich nach ihrem Einsatzbereich. So soll etwa der Einsatz in Bereichen wie kritischer Infrastruktur (Verkehr), Ausbildung, Zugang zu Sozialleistungen oder wichtigen privaten Dienstleistungen oder die Verwaltung der Justiz nur unter bestimmten, hohen Anforderungen zulässig sein. Diese werden in über 40 Artikeln genauer festgelegt und umfassen strenge Vorgaben an das Risikomanagement, die Dokumentation der Entwicklung, Qualität der Datensätze, Transparenz, Kontrolle und menschliche Überwachung der Systeme. Unter anderem müssen die Anwendungen vor der Marktzulassung eine Konformitätsprüfung unterlaufen und eine entsprechende Zertifizierung erhalten.
- KI mit **geringem oder minimalem Risiko**: Die Anforderungen an andere KI mit minimalem oder geringem Risiko sind deutlich geringer. Aber auch für diese sieht der Kommissionsvorschlag klare Transparenz- und Anzeigepflichten vor, insbesondere, wenn die KI gegenüber Menschen eingesetzt werden soll.

Aufsicht, Sandboxes und Sanktionen

Die Mitgliedstaaten sollen gesonderte Aufsichtsbehörden schaffen, die mit der Überwachung und Aufsicht der KI-Hersteller und Produkte betraut sind. Deren Tätigkeit soll im European Artificial Intelligence Board auf europäischer Ebene koordiniert werden. Auch hierin gleichen die Regelungen der KI-Verordnung der DSGVO. Die aus der DSGVO bekannten hohen Bußgelder von bis zu 4% des Jahresumsatzes eines Unternehmens oder 20 Millionen Euro werden durch die KI-Verordnung, die Bußgelder i.H.v. 30 Millionen Euro oder 6% des globalen Jahresumsatzes vorsieht, noch übertroffen. Und ein weiterer wichtiger Unterschied besteht zur DSGVO: die Datenschutzvorgaben richten sich nicht unmittelbar an Hersteller von Anwendungen (Soft- oder Hardware), sondern nur an die

Anwender. Der KI-Verordnungsentwurf adressiert die Pflichten dagegen ausdrücklich auch an Hersteller von Anwendungen.

Eine Möglichkeit für die Hersteller, solche Sanktionen zu vermeiden, ist die Durchführung ausführlicher Tests, bevor die Technik der Öffentlichkeit zugänglich gemacht wird. Deshalb ermutigt der KI-Verordnungsentwurf die Mitgliedstaaten, Vorgaben für sogenannte Sandkästen („Sandboxes“) zu schaffen, in denen KI-Produkte bei kontrollierten Bedingungen getestet werden können.

Zu streng oder nicht streng genug – Kritik von allen Seiten

Natürlich bleibt angesichts des regulatorischen Neulandes mit umfangreichen und bußgeldbewährten Pflichten die Kritik nicht aus. Zwar scheint man sich überwiegend einig zu sein, dass die Regulierung von KI sinnvoll ist und der Entwurf der KI-Verordnung ein wesentlicher Schritt in die richtige Richtung ist, zumal die EU hier eine zu begrüßende Vorreiterrolle einnimmt. Angesichts des risikobasierten Ansatzes werden aber Befürchtungen laut, dass die EU-Kommission den angestrebten Spagat zwischen Innovationsförderung und Schutz wesentlicher Rechtsgüter jedenfalls mit diesem Entwurf nicht meistern kann.

Die einen befürchten, dass die umfassenden Regelungen und Sanktionen des Verordnungsentwurfs entwicklungshemmend wirken. Laut Handelsblatt kann bei einer zu strengen Regulierung ein Wettbewerbsnachteil für europäische Unternehmen gegenüber Konkurrenten aus China und den USA entstehen. Auch unabhängig davon könnten die umfassenden Verpflichtungen des Verordnungsentwurf auf Entwickler abschreckend wirken – zu erwarten seien daher hohe Entwicklungskosten für europäische KI, wie etwa der Onlinenachrichtendienst lto.de in der Berichterstattung zum Entwurf herausstellte. Dabei wird unter anderem auch kritisiert, dass die Verordnung den Begriff KI sehr weit definiere – so seien faktisch alle softwarebasierten Technologien erfasst, die heute das Internet ausmachen, wie Industrievertreter gegenüber dem Handelsblatt erklärten. Die EU-Kommission selbst geht laut ihrer Pressemitteilung davon aus, dass für den Großteil der Anwendungen, die unter die KI-Definition fallen, auch mit der KI-Verordnung keine strengeren Anforderungen als nach bereits geltendem Produktsicherheitsrecht aufgestellt werden.

Anderen wiederum geht der Vorschlag nicht weit genug: Wie das Nachrichtenmagazin Der Spiegel berichtet, sind etwa nach Auffassung der europäischen Bürgerrechtsorganisation EDRi die Ausnahmen für den Einsatz von biometrischer Identifikationssoftware zu weit gefasst. Auch das Handelsblatt berichtet von Kommentatoren, die bemängeln, dass der Entwurf den Einsatz von Datensätzen, die zu diskriminierenden Ergebnissen führen, nicht hinreichend verhindern würde. Auch insofern wird Nachbesserungsbedarf gesehen.

Internationale Beachtung

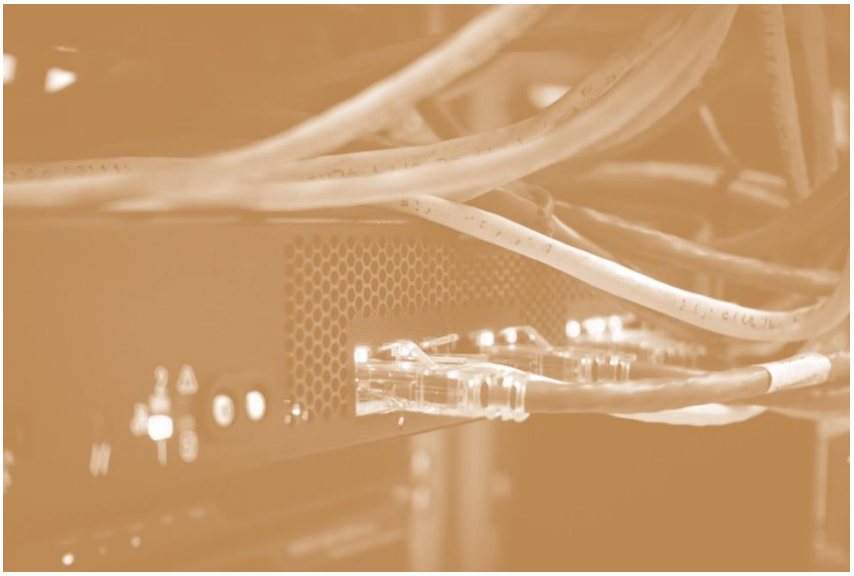
Dabei betritt die EU mit einem so umfassenden Vorschlag zur Regulierung von KI regulatorisches Neuland – weltweit existiert bisher nichts Vergleichbares. Auch deshalb wird dem Verordnungsentwurf international viel Aufmerksamkeit geschenkt. Viele erwarten, dass die KI-Verordnung das Vorbild für den neuen Regulierungsstandard bilden wird – ähnlich wie die DSGVO weltweiter Maßstab für die Regulierung personenbezogener Daten geworden ist (so die Erwartung des Nachrichtenmagazins The Economist: „Brüssel Effekt").

Dass der KI-Verordnung internationale Beachtung zukommt, hat aber auch einen anderen Grund: Ähnlich wie die DSGVO setzt auch die KI-Verordnung auf das sogenannte Marktort-Prinzip: Konkret heißt dies, dass nicht nur Hersteller und Entwickler erfasst sind, die einen Sitz in Europa haben, sondern die Vorgaben der KI-Verordnung für alle gelten, die ihre Produkte auf den europäischen Markt bringen wollen. Damit spielt der Ausgang des europäischen Gesetzgebungsprozesses auch für außereuropäische Entwickler eine wichtige Rolle.

Weiterer Gang: Beratung des Europäischen Parlaments

Mit den inhaltlichen Fragen wird sich nun das Europäische Parlament beschäftigen dürfen, an das die Kommission ihren Entwurf zur Beratung weitergeleitet hat. Wann und in welcher Form dann die endgültige Fassung der KI-Verordnung vorliegt, ist schwer vorauszusagen. Bis dahin erwarten die Berichterstatter der Wirtschaftswoche eine „Lobbyschlacht" der verschiedenen Interessengruppen um die genauen Regelungen. Ob das tatsächlich der Fall sein wird, bleibt abzuwarten – jedenfalls erscheint es angesichts der Fülle der Regelungen und der Relevanz der

betroffenen Interessen und Rechte unwahrscheinlich, dass es vor dem nächsten Jahr zur Verabschiedung der Verordnung kommen wird. Wir werden berichten.



Kommt jetzt endlich die ePrivacy-Verordnung?

Nach Jahren des Wartens und der Unstimmigkeiten nun der nächste Schritt in Sachen ePrivacy-Verordnung: Im Februar 2021 konnte sich der EU-Ministerrat auf eine Version einigen, an die sich jetzt Beratungen von Rat, Kommission und Parlament der Europäischen Union anschließen können. Wir stellen für Sie dar, was vor allem in Bezug auf den Einsatz von Cookies & Co. vorgesehen ist und wie dies für Online-Angebote auf der eigenen Website adaptiert werden kann.

Bereits seit April 2016 wird die EU-weite ePrivacy-Verordnung zugunsten eines vereinheitlichten Binnenmarkts diskutiert. Für Verbraucher soll sie eine Stärkung der Privatsphäre und eine intensivere Regulierung des Datenschutzes mit sich bringen – und endlich eine Verzahnung mit der DSGVO. Bereits 2017 legte die EU-Kommission den ersten Entwurf vor. Obwohl die ePrivacy-Verordnung ursprünglich gemeinsam mit der DSGVO im Frühjahr 2018 in Kraft treten sollte, konnten sich die Mitgliedsstaaten seither nicht auf eine gemeinsame Linie einigen. Mit dem im EU-Ministerrat

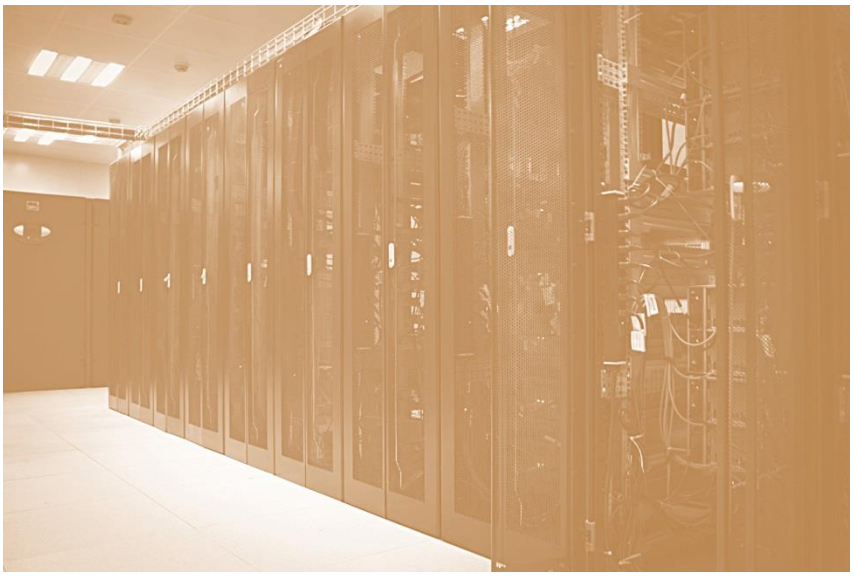
nun angenommenen Entwurf vom 10.02.2021 werden neue Hoffnungen auf eine baldige Einigung geweckt.

In Sachen Cookies & Co. zeigt sich auch der neue Entwurf strikt: Der Zugriff auf Endgeräte – sei es über Cookies oder andere Techniken – und die Informationsbeschaffung über derartige Zugriffe ist grundsätzlich verboten und nur ausnahmsweise zulässig. Die Ausnahmen sind abschließend gefasst und orientieren sich an der bisherigen, spätestens seit Sommer 2020 auch in Deutschland geltenden Rechtslage. Zu begrüßen ist indes, dass sie deutlich konkreter gefasst sind als nach aktuell geltendem Recht – und gegenüber zwischenzeitlich kursierenden Verordnungsentwürfen auch deutlich weiter. Ohne Einwilligung der Nutzer soll danach der Endgerätezugriff insbesondere in folgenden Fällen erlaubt sein:

- Erforderlich für die Bereitstellung / Erbringung eines Dienstes
- Reichweitenmessung durch den Anbieter des Dienstes oder einen Dritten, der als Auftragsverarbeiter oder gemeinsam Verantwortlicher eingebunden ist
- Aufrechterhaltung oder Wiederherstellung der Sicherheit der Dienste einschl. Betrugsverhinderung, Erkennen von technischen Störungen
- Erforderlich für ein Software-Update (Sicherheitsgründe, nach vorheriger Information und mit der Möglichkeit, die Aktualisierung zu verhindern oder abzuschalten)
- Ortung bei Notrufen
- Kompatible Zwecke unter engen Voraussetzungen

Um eine verbesserte Nutzerfreundlichkeit zu erreichen, sollen künftig sog. „Whitelisting-Angebote“ ermöglicht werden: Durch Voreinstellungen im Browser werden Consent Management Tools auf den einzelnen Websites damit obsolet. Nutzer können damit das „Durchklicken“ von unzähligen Consent Management Tools auf jeder einzelnen Website vermeiden – sicherlich birgt dies indes erhebliche Risiken für die Conversion Rates der einzelnen Websites.

Ob sich dieser Entwurf nun durchsetzen, bleibt indes ungewiss. Gerade der Einsatz von Cookies zu Werbezwecken wird von Parlament und Rat kontrovers angegangen – die Diskussionen hierzu werden wir weiterverfolgen und darüber berichten.



Update: Social Media und Datenschutz

WhatsApp ändert seine AGB nun doch – der Datenaustausch mit Facebook wird damit zur Pflicht. Anfang des Jahres war dieser Schritt noch aufgrund erheblicher Proteste zurückgestellt worden. Parallel dazu hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) eine Anordnung erlassen, die es der Facebook Ireland Ltd. verbietet, personenbezogene Daten von WhatsApp zu eigenen Zwecken zu verarbeiten. Und auch an anderen Stellen wird die Datenschutzkonformität von Facebook & Co. aktuell wieder brisant diskutiert, Anfang April etwa ist ein Datenschutzleck bei Facebook bekannt geworden, über das personenbezogene Daten von mehr als einer halben Milliarde Menschen veröffentlicht wurden. Grund genug für einen aktuellen Überblick über die wichtigsten Diskussionen rund um die Vereinbarkeit der Social Media Angebote mit dem Datenschutz.

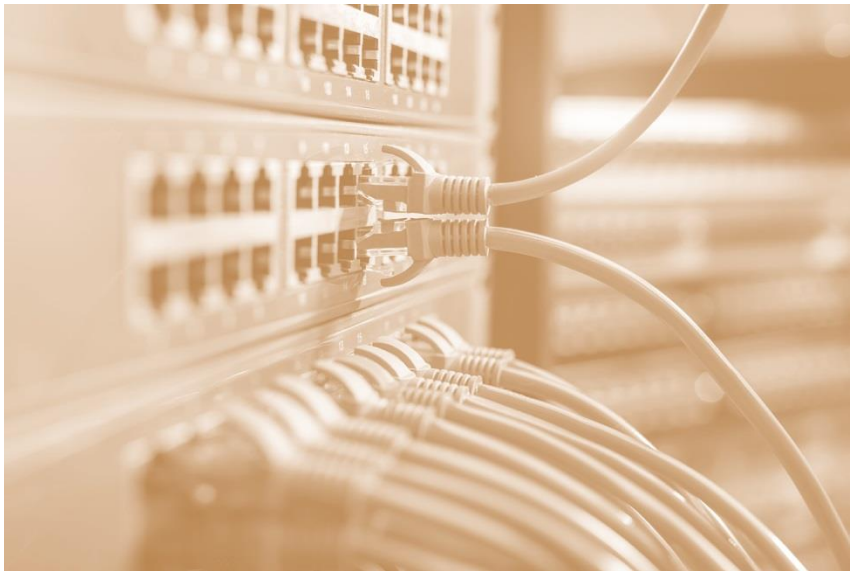
Anfang April sind aufgrund eines Datenlecks personenbezogene Daten von knapp einer halben Milliarde Facebook-Nutzern im Netz aufgetaucht. Hierunter waren nicht nur E-Mail-Adressen, sondern unter anderem auch Telefonnummern, die mit den betroffenen Konten verknüpft waren. Akute Folge sind SMS-Spamwellen, Phishing-Betrugsversuche und zum Teil Mobbing-Nachrichten. Eine Information der Betroffenen seitens Facebook erfolgte nicht. Das Unternehmen berief sich darauf, dass es sich bei dem Datenleck um ein altes, bereits bekanntes Leck handele.

Eine Informationspflicht gem. Art. 34 DSGVO bestehe daher nicht.

Ähnlich wie bei Facebook sind Anfang des Jahres auch größere Datenmengen von LinkedIN und der Anwendung Clubhouse im Internet aufgetaucht. Betroffen sind Daten wie IDs, Klarnamen, E-Mail-Adressen und Handynummern.

Ungeachtet der Datenpannen ändert WhatsApp zum 15.05.2021 seine Nutzungsbedingungen und lässt sich umfangreiche Einwilligungen zum Transfer von Daten an Facebook-Unternehmen verpflichtend einräumen. Hiergegen eröffnete die Hamburgische Datenschutzbehörde (HmbBfDI) ein Dringlichkeitsverfahren gem. Art. 66 DSGVO, das vor wenigen Tagen in die Untersagung der Weiterverarbeitung mündete. Der HmbBfDI sieht keine ausreichende Rechtsgrundlage für die Verarbeitung der WhatsApp-Nutzerdaten durch Facebook. Die von den Nutzern erteilte Einwilligung ist nach Auffassung der Behörde mangels Freiwilligkeit unwirksam, da die weitere Nutzung von WhatsApp nur möglich ist, wenn eine Einwilligung in den Datentransfer zu Facebook-Unternehmen erteilt wird. Eine entsprechende Einwilligung sei nicht "freiwillig", da die Nutzer, wenn sie nicht einwilligen, damit rechnen müssen, WhatsApp nicht mehr nutzen zu können.

Die Anordnung ist sofort vollziehbar, gilt also nunmehr ungeachtet eines möglichen (gerichtlichen) Vorgehens dagegen. Allerdings ist sie im Dringlichkeitsverfahren zeitlich beschränkt und verfällt nach drei Monaten. Der HmbBfDI dringt daher nunmehr auf eine EU-weite Lösung und beantragt eine Befassung des Europäischen Datenschutzausschusses mit dem Thema. Primär für Facebook Ireland Ltd. zuständig ist die irische Datenschutzaufsichtsbehörde, die indes zuletzt weniger aktiv war.



Schrems II – ein Hilferuf der deutschen Wirtschaft

Kaum ein Thema treibt die Datenschutzwelt derzeit so um wie der transatlantische Datentransfer. Zur Erinnerung: Der EuGH hatte mit seinem Urteil in Sachen „Schrems II" die Debatte um die Zulässigkeit eines Datentransfers von der EU in die USA erneut befeuert. Das EU-US-Privacy Shield, das die rechtliche Zulässigkeit absichern sollte, wurde für unwirksam erklärt und auch die anderen rechtlichen Möglichkeiten aus dem Instrumentenkasten der DSGVO (u.a. die Standardvertragsklauseln) wurden mit Fragezeichen versehen. In der EU ansässige Unternehmen jeglicher Größenordnung bangen seither um die Zulässigkeit einzelner Verarbeitungsvorgänge oder ganzer Geschäftsmodelle.

Anfang Mai wurde darüber berichtet, dass sich zahlreiche deutsche Unternehmen, darunter auch große Konzerne, mit einem Hilferuf an die Bundesregierung gewandt haben. Anlass dafür war und ist die fortdauernde Rechtsunsicherheit beim Datentransfer in die USA. Auf diesen sind praktisch alle Unternehmen bei ihrer täglichen Arbeit angewiesen, sei es bei Cloud-Lösungen oder gerade in der Pandemie mit Produkten wie Microsoft Teams oder Zoom oder etlichen anderen US-basierten Digitalangeboten. Die deutschen Unternehmen befürchten konkret Untersagungen und im schlimmsten Fall hohe Bußgelder, sehen aber gleichzeitig keine technische Alternative zu weltweit verbreiteten Produkten und Cloud-Lösungen der großen US-Anbieter. Eine klassische Zwickmühle. Die Datenschutzaufsichtsbehörden werden denn auch

zunehmend aktiv und beginnen mit ersten Schwerpunktprüfungen. Die Initiative und der „Hilferuf“ zeigen, dass Unternehmen jeglicher Größenordnung intensiv mit dem gleichen Problem ringen. Gleichzeitig scheint eine Lösung noch in weiter Ferne.

Was tut die Politik?

Bekannt ist, dass die EU und die (neue) US-amerikanische Administration das Thema auf dem Schirm haben und offenbar an einer politischen Lösung arbeiten. Wie diese aussehen kann, ist allerdings noch unklar. Man hört derzeit von einer Ausweitung der Rechtsschutzmöglichkeiten für EU-Bürger in den USA. Ob das allerdings praktikabel und effektiv ist, bleibt abzuwarten. Auch wenn die EU-Kommission über intensivierte Bemühungen einer Lösungsfindung mit den USA berichtet, dürfte eine kurzfristige Lösung kaum realistisch sein. Selbst wenn eine zeitnahe politische Lösung zwischen der EU und den USA gefunden wird, bleibt abzuwarten, ob diese die dann absehbare Entscheidung „Schrems III“ überlebt.

Was tun die Behörden? Was tun Wettbewerber?

In Deutschland verhalten sich die Datenschutzbehörden unterschiedlich, indes ist eine zunehmende Aktivität zu beobachten: Vermehrt werden Prüfungen durchgeführt oder angekündigt, etwa als „Stichprobenkontrollen“ oder Schwerpunktprüfungen. Die Behörden gehen noch davon aus, dass derzeit die Standardvertragsklauseln genutzt werden können, allerdings nur nach Einzelfallprüfung und mit Bezug auf die USA zudem nur mit zusätzlichen Schutzmaßnahmen. So obliegt es den Unternehmen, das gleichwertige Datenschutzniveau in den USA (und anderen Drittstaaten) zu prüfen und zu bewerten – fehlt die Einzelfallprüfung, reicht schon dies nach einer aktuellen Entscheidung der BayLDA in Sachen MailChimp für eine Untersagung. In der Praxis erfolgt dies zumeist durch Fragebögen oder sonstige Anfragen bei den jeweiligen US-Anbietern. Besonders streng gehen etwa die Datenschutzbehörden in Berlin und Hamburg vor, auch im Westen sind etwa in Rheinland-Pfalz zunehmende Aktivitäten zu beobachten. Es wird gefordert, dass die verantwortlichen Unternehmen sich im Detail mit der Rechtslage in den USA auseinandersetzen und Zusatzvereinbarungen treffen, die die Datensicherheit gewährleisten. Die Behörden betonen in diesem

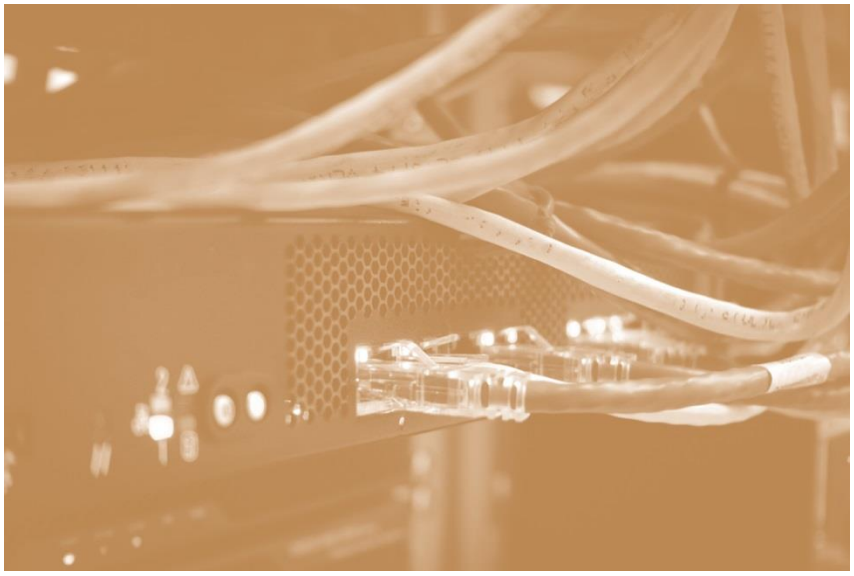
Zusammenhang mitunter, dass dies wohl nur in wenigen Ausnahmefällen erfolgreich sein könne.

Angemessene Garantien müssen indes für einen Drittstaatentransfer stets gefunden werden, um nicht offensichtlich gegen die DSGVO zu verstoßen und dann u.U. sogar ein Strafbarkeitsrisiko zu begründen. Zu prüfen sind daher neben den Standardvertragsklauseln, die für den US-Transfer zusätzlicher Schutzmaßnahmen bedürfen, auch alternative Lösungen wie beispielsweise Einwilligungen konkret in den US-Transfer. Die pauschale Unterzeichnung von Standardvertragsklauseln ohne zusätzliche Maßnahmen stellt jedenfalls keinen Freibrief für den US-Datentransfer dar.

Wettbewerbsrechtliche Abmahnungen scheinen in dem Bereich hingegen kaum von Relevanz zu sein, vermutlich deswegen, weil nahezu alle Unternehmen auf IT-Lösungen und Produkte von US-Anbietern angewiesen sind.

Monitoring und Exit-Strategie

Für Unternehmen bleibt derzeit nur eine unbefriedigende Lösung, wenn sie nicht auf sämtliche IT-Anwendungen von US-Anbietern verzichten wollen. Sie müssen die Drittstaatentransfers im Unternehmen identifizieren, prüfen und für geeignete Garantien sorgen, oftmals helfen hier auch Risikoabwägungen und die Prüfung alternativer Wege, etwa über die Einwilligung. Dass dieser Prozess nicht kurzfristig zu erledigen ist, betonen in inoffiziellen Gesprächen auch die Aufsichtsbehörden. Jedenfalls ist angesichts dessen anzuraten, das Thema aktiv anzugehen und zudem die aktuellen Entwicklungen und die Aktivität der für das jeweilige Unternehmen zuständigen Behörde zu verfolgen. Unternehmen sollten ggf. rechtzeitig auch über eine Exit-Strategie nachdenken, also ggf. den Verzicht auf Anwendungen und die Migration zu alternativen Optionen.



Zu guter Letzt

Diesen Monat gab es nicht nur interessante Entscheidungen zur Frage des Rechtsmissbrauchs bei einem geltend gemachten Auskunftsanspruch, sondern es wurden auch wieder Bußgelder wegen Verstoßes gegen die Datensicherheit verhängt. Außerdem teilt das BSI mit, dass es Hilfsmittel zu Verteidigung von IT-Systemen mit Windows 10 zur Verfügung stellt.

- **Deutschland: Auskunftsanspruch auch bezüglich der Kopie von personenbezogenen Daten?**

Das Bundesarbeitsgericht (BAG) beschäftigte sich jüngst mit der Reichweite des Auskunftsanspruchs gem. Art. 15 DSGVO. Zusätzlich zu einer Auskunft zu seinen personenbezogenen Daten machte ein Arbeitnehmer einen Anspruch auf eine Kopie aller verarbeiteten personenbezogenen Daten inklusive des zwischen Arbeitgeber und Arbeitnehmer geführten E-Mail-Verkehrs sowie der E-Mails, in denen er genannt wurde, geltend. Art. 15 Abs. 3 DSGVO verpflichtet Verantwortliche auch dazu, „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen“. Das BAG umging nun in seinem Urteil vom 27.04.2021 eine Beantwortung dieser inhaltlichen Frage: Es ließ den Klageantrag bereits in der Zulässigkeit daran scheitern, er sei zu unbestimmt. Notwendig sei es, klarzustellen, auf welche E-Mails sich das Klagebegehren bezieht, nicht nur pauschal auf Kopien „des E-Mail-Verkehrs“. Sei eine hinreichende Bestimmung für den Kläger

nicht möglich, müsse eben im Wege der Stufenklage zunächst Auskunft verlangt werden.

- **Niederlande: Kein Auskunftsrecht bei Rechtsmissbrauch**

In den Niederlanden hat ein Gericht jüngst ein Auskunftsrecht wegen missbräuchlicher Geltendmachung abgelehnt: Es sei dem Betroffenen lediglich darum gegangen, ein Verfahren einzuleiten, um von den Verantwortlichen Schadensersatz zu erhalten, wenn deren Antworten auf seine Anträge verspätet waren. Ein solches Verlangen sei auch nicht durch die DSGVO geschützt.

- **BSI stellt Sicherheitseinstellungen für Windows 10 zur Verfügung**

Das Bundesamt für Sicherheit in der Informationstechnik hat im Mai hilfreiche Sicherheitshinweise für die Konfiguration von Microsoft Windows 10 zum Download bereitgestellt. Viele Angriffe ließen sich bereits mit den im Betriebssystem vorhandenen Bordmitteln erkennen und verhindern, wenn die Konfiguration korrekt gewählt würde.

- **Spanien: 1,5 Mio. Euro wegen Verstoßes gegen die Informationspflicht und Datensicherheit**

Ein spanischer Energieversorger hatte Vertragsabschlüsse über diverse Medien wie Telefonhotlines oder Website-Formulare vorgenommen, ohne die Betroffenen – nach Ansicht der Aufsichtsbehörde – ordnungsgemäß nach Art. 13 DSGVO zu informieren. Insbesondere fehlte es an einer Aufklärung über die Betroffenenrechte, die Angaben zum Verantwortlichen waren unvollständig, wodurch eine weitere Kontaktaufnahme erschwert wurde. Die Verteidigung, diese Informationen seien an anderer Stelle durch einfache Suchanfrage zugänglich gewesen, wurde als nicht ausreichend zurückgewiesen.

Trotz mehrerer Sanktionen hatte das Unternehmen seine Prozesse nicht an die gesetzlichen Vorgaben angepasst, sodass es insgesamt wegen Verstoßes gegen Art. 13 DSGVO und gegen Art. 25 DSGVO zu einem Bußgeld i.H.v. 1,5 Mio. Euro kam.

- **Spanien: 1 Mio. Euro-Bußgeld gegen spanischen Finanzdienstleister**

Gegen den spanischen Finanzdienstleister EQUIFAX IBÉRICA S.L. wurde ein Bußgeld i.H.v. 1 Mio. Euro erlassen. Das Unternehmen habe Daten von Personen in ein eigenes Verzeichnis aufgenommen, gegen die seitens öffentlicher Institutionen Beschwerden, ausstehende Schulden oder andere rechtliche Ansprüche vorlagen. Anhand dieser Daten schätzten Banken die Kreditwürdigkeit von Personen ein. Die Verarbeitung war nach Ansicht der Aufsichtsbehörde insgesamt datenschutzrechtswidrig. Zusammengetragen hatte das Unternehmen die Daten aus behördlichen Veröffentlichungen. Hierunter befanden sich auch Daten zu Schulden, die nicht mehr existierten. Die Richtigkeit und Aktualität dieser Angaben habe EQUIFAX indes nicht hinreichend überprüft.

- **Norwegen: 2,5 Mio. Euro-Bußgeld wegen unzulässigem Werbe-Tracking**

Das amerikanische Unternehmen Disqus stellte einer Reihe norwegischer Online-Zeitungen eine Plattform zum Teilen von öffentlichen Online-Kommentaren zur Verfügung und ist außerdem im Bereich der programmatischen Werbung tätig. Aufgrund eines Artikels des Norwegischen Rundfunks besah sich die Norwegische Datenschutzbehörde die Angelegenheit genauer und verhängte gegen das Unternehmen in der Folge ein Bußgeld in Höhe von 2,5 Mio. Euro. Disqus führe ein unrechtmäßiges Tracking von Besuchern norwegischer Websites durch und habe deren Daten rechtswidrig an dritte Werbepartner weitergegeben. Das Interesse von Disqus an der Bereitstellung von verhaltensorientiertem Online-Marketing könne die negativen Auswirkungen des groß angelegten Profilings bei Weitem nicht überwiegen, so dass das Vorgehen nicht aus berechtigten Unternehmensinteressen heraus erlaubt sei – ohne Einwilligung fehlte es nach Behördenansicht an einer Erlaubnisgrundlage.

- **Niederlande: Bußgeld wegen Wifi-Trackings in der Innenstadt**

Aufgrund datenschutzverletzender Vorgehensweise der Gemeinde Enschede bei der Installation eines 24/7-WiFi-Tracking-Systems im Zentrum der Stadt wurde diese mit einem Bußgeld in Höhe von

600.000 Euro belegt. Ziel des Trackings war es, die Effektivität der kommunalen Investitionen zu messen. Die Aufsichtsbehörde sah hierfür indes keine Erlaubnisgrundlage. Die Verteidigung der Stadt, durch ein Abschneiden eines Teils der gehashten MAC-Adresse seien die Daten ausreichend anonymisiert, wurde zurückgewiesen: in Kombination mit den anderen verarbeiteten Daten sei das Risiko des Rückschlusses auf die Identität einer Person zu hoch, um einen Personenbezug abzulehnen. Angesichts der umfangreichen Tracking-Daten könne ein eindeutiges Lebens- und Standortmuster abgeleitet werden, welche bspw. den Wohn- oder Arbeitsort einer Person offenbart.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de