LOSCHELDER

Newsletter Datenschutzrecht
November 2023

Sehr geehrte Damen und Herren,

das Jahr neigt sich dem Ende zu und bringt in den letzten Wochen nochmals viel Schwung in die Datenwirtschaft: Das Europäische Parlament hat am Donnerstag, den 9. November, den Data Act verabschiedet und einige erwarten gar noch eine Einigung zum AI-Act. Diese könnte am 6. Dezember gelingen. Ob dies der Fall sein wird, ist allerdings noch völlig offen.

Doch auch altbekannte Themen sind aktuell wieder auf der Agenda: Der erst kürzlich veröffentlichte Angemessenheitsbeschluss für Datenübermittlungen in die USA, das EU US-Data Privacy Framework, hat eine erste Gerichtsrunde überstehen müssen. Auch die (behördlichen) Überprüfungen von ChatGPT gehen weiter. Schließlich hat der EuGH zwei weitere datenschutzrechtlich hoch spannende Entscheidung verkündet, zum Identitätsdiebstahl i.S.d. DSGVO und zum Begriff der personenbezogenen Daten und der Verarbeitungserlaubnis „gesetzliche Verpflichtung“.

Zu guter Letzt stellen wir Ihnen einige interessante Vorgänge im Datenschutzrecht vor. So wurde etwa ein Datenleck bei Microsoft entdeckt, personalisierte Werbung auf Facebook und Instagram soll nun europaweit verboten werden und Meta hat ein neues Geschäftsmodell eingeführt.

Wir freuen uns über Ihr Interesse!

Inhalt

US-Datentransfer: Sitzt, passt, wackelt und hat Luft?

Seit Juli gilt der neue Angemessenheitsbeschluss für den Datentransfer in die USA, das EU US-Data Privacy Framework. Kritik hieran war schon früh zu hören. Wenig überraschend sind erste Verfahren anhängig. Überraschend ist dagegen: Es gab sogar bereits erste Gerichtsentscheidungen. Also: Gilt das EU US-DPF noch oder wackelt der US-Datentransfer schon wieder?

Seit dem 10. Juli 2023 ist das EU US-Data Privacy Framework (DPF), der neue Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO, in Kraft. Personenbezogene Daten können darunter sicher an zertifizierte Unternehmen übermittelt werden. Ob ein Unternehmen zertifiziert ist, sollte stets aktuell überprüft werden (hier). Wir haben darüber in unserem Newsletter an dieser Stelle berichtet.

Der Beschluss attestiert ein angemessenes Schutzniveau, vergleichbar mit dem der Europäischen Union, für personenbezogene Daten, die auf der Grundlage des DPF aus der EU an unter dem DPF zertifizierte US-Unternehmen übermittelt werden. Neu ist dabei unter anderem die Einrichtung eines US-Gerichts („Data Protection Review Court"), an das sich EU-Bürger mit Beschwerden über den Zugriff auf ihre Daten durch US-Sicherheitsbehörden wenden können. Für die Übermittlung an nicht zertifizierte Unternehmen muss weiterhin auf die bekannten Mittel wie Standardvertragsklauseln oder Binding Corporate Rules zurückgegriffen werden (Art. 46, 47 DSGVO), regelmäßig notwendigerweise ergänzt um zusätzliche Maßnahmen.

Angemessenheitsbeschluss schon wieder in Gefahr?

Noch vor Erlass des DPF brandete bereits Kritik an diesem auf. In der öffentlichen Diskussion wurde es teils als bloße Kopie des 2020 durch den EuGH für unwirksam erklärten EU-US Data Privacy Shield bezeichnet. So überraschte es kaum, dass der neue Angemessenheitsbeschluss zeitnah bei den europäischen Gerichten landen würde. Die erste Klage gegen das DPF liegt vor. Der EU-Parlamentarier Philippe Latombe hat beim EuG Klage gegen den Beschluss der EU-Kommission zum Data Privacy Framework eingereicht, siehe hier seine Pressemitteilung (französisch). Er klagte auf Nichtigerklärung des DPF und verfolgt mit einem Antrag im einstweiligen Rechtsschutz dessen Aussetzung. Auch eine

Einschaltung des EuGH – über nationale Gerichte – ist nur eine Frage der Zeit. NOYB rechnet nach eigenen Angaben mit einem Verfahren vor dem EuGH Anfang 2024. Wie die Gerichte indes entscheiden, ist völlig offen.

Erste Eilverfahren erfolglos

Bemerkenswert ist, dass ein erstes Eilverfahren gegen das DPF bereits erfolglos geblieben ist: Das EuG hat mit Beschluss vom 12. Oktober 2023 (Rs. T-553/23 R) den Antrag auf einstweilige Anordnung zurückgewiesen. Das DPF bzw. sein Vollzug wird nicht vorläufig ausgesetzt, sondern gilt bis zum Abschluss des Hauptsacheverfahrens. Dies ist ein erster Fingerzeig dahin, dass das EuG jedenfalls keine offensichtliche Unwirksamkeit sieht.

Anzuerkennen ist allerdings auch, dass die Hürden für eine solche einstweilige Anordnung im EU-Recht hoch sind. Die beantragte Anordnung muss sachlich und rechtlich „auf den ersten Blick" gerechtfertigt (*fumus boni juris*) und dringend sein, also ohne Anordnung müssen schwere und nicht wiedergutzumachende Schäden drohen.

Dennoch ist die Entscheidung ein erster Fingerzeig dahin, dass das DPF von den Europäischen Gerichten jedenfalls nicht als „bloße Kopie" des EU US-Privacy Shields gesehen wird, sondern es einer genaueren Würdigung bedarf.

Praxis bleibt vorerst sicher

Für die Praxis gilt ohnehin: Das DPF behält so lange Gültigkeit – und kann von Unternehmen für Datenübermittlungen in die USA herangezogen werden – bis es durch Entscheidung des EuGH für unwirksam erklärt wurde. Für die Unternehmenspraxis bedeutet dies also erst einmal Ruhe.

Allerdings ist Unternehmen zu raten, die Entwicklung im Auge zu behalten und insbesondere bei der Implementierung von Anwendungen, aus denen sich die Migration zu anderen Anbietern als schwierig gestaltet, zu bedenken, dass das DPF in einiger Zeit wieder kippen könnte. Ob das aber passiert, ist noch völlig offen.

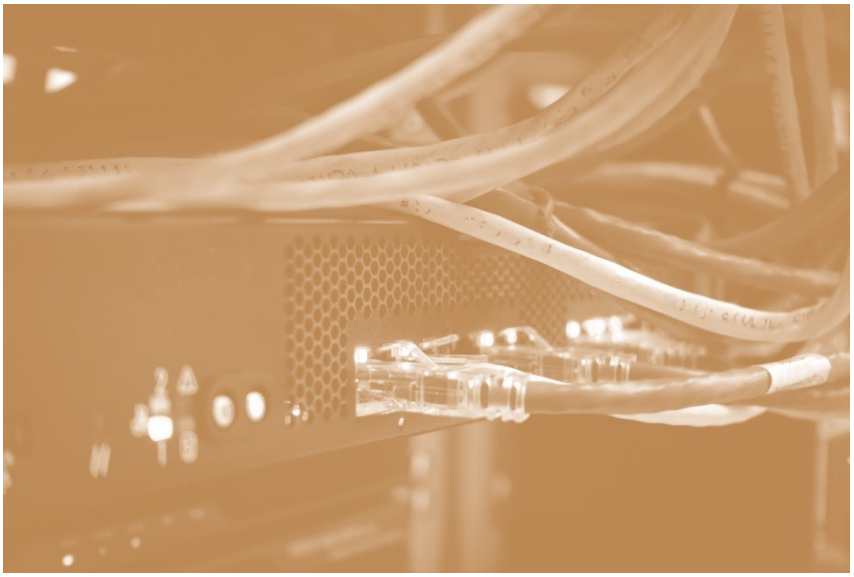
Datenschutzbehörden nehmen ChatGPT gründlich unter die Lupe

Ob ChatGPT DSGVO-konform arbeitet, wird nach wie vor durch die deutschen Datenschutzbehörden umfassend geprüft. Die Antworten des ChatGPT-Betreibers OpenAI auf einen Fragekatalog der Datenschutzbehörden hat neue Fragen aufgeworfen, die die Datenschutzbehörden nun zu klären versuchen.

Nachdem Italien ChatGPT im Frühjahr sperrte – wir berichteten hierüber an dieser Stelle – haben deutsche Datenschutzbehörden ein Auskunftsersuchen an OpenAI geschickt. Mittlerweile wurden die dort gestellten Fragen beantwortet, aus Sicht der Datenschutzbehörden ergaben sich aber weitere Nachfragen. Prof. Dr. Dieter Kugelmann, Leiter der bei der Datenschutzkonferenz eingerichteten Taskforce „Künstliche Intelligenz“, hat einen neuen Fragebogen zum KI-Sprachmodell entwickelt, welchen mehrere deutschen Datenschutzbehörden an OpenAI gesendet haben. Er betont die Notwendigkeit der Transparenz von Künstlicher Intelligenz – sie müsse nachvollziehbar und erklärbar sein, damit sie kontrolliert und an den Normen und Werten der Gesellschaft gemessen werden kann. Im neuen Fragebogen geht es insbesondere darum, ob die Verarbeitung personenbezogener Daten durch ChatGPT rechtmäßig erfolgt. Besondere Aufmerksamkeit bekommen hierbei die besonderen Datenkategorien nach Art. 9 DSGVO, zu denen u.a. Gesundheitsdaten gehören. Zudem soll

geklärt werden, ob OpenAI den Betroffenenrechten auf Auskunft, Berichtigung sowie Löschung der personenbezogenen Daten ausreichend nachkommt. Auch möchte die Datenschutzkonferenz mithilfe des Fragebogens herausfinden, ob ChatGPT personenbezogene Daten zuverlässig erkennt und wie es eine datenschutzkonforme Verarbeitung der personenbezogenen Daten sicherstellt.

Solange OpenAI keine Niederlassung in der EU hat, sind alle Datenschutzbehörden der Mitgliedsstaaten gleichermaßen für die Einhaltung der DSGVO zuständig. Da sich die datenschutzrechtliche Bewertung auf den gegenwärtigen sowie vergangenen Zustand bezieht, würde das Prüfverfahren auch nicht enden, sollte sich OpenAI etwa in Irland niederlassen. Zudem sind die deutschen Aufsichtsbehörden weiterhin (in Kooperation mit der Aufsichtsbehörde am Ort der Hauptniederlassung) zuständig soweit ChatGPT in Deutschland angeboten wird.



EuGH: Immaterieller Schadensersatz und Identitätsdiebstahl

Liegt bereits ein Identitätsdiebstahl i.S.d. DSGVO vor, wenn Hacker personenbezogene Daten entwendet haben, aber sich (bisher) nicht als die betroffene Person ausgegeben haben? Diese und andere Fragen zum Verständnis von immateriellem Schadensersatz und seiner Beurteilung stellte sich das Amtsgericht München und legte sie im Rahmen eines Vorabentscheidungsverfahrens dem EuGH vor. Der Generalanwalt beim EuGH hat sich Ende Oktober zu der Frage geäußert, wann ein Identitätsdiebstahl vorliegt.

In den letzten Monaten konkretisierte der EuGH die Voraussetzungen, die für die Gewährung vom immateriellen Schadensersatz nach Art. 82 DSGVO erforderlich sind – wir berichteten u.a. an dieser Stelle und auch hier im Überblick. Die Aussagen des EuGH zur Gewährung eines immateriellen Schadensersatzes waren auf Stufe der Schadenshöhe im Wesentlichen Folgende:

1. Der Eintritt eines materiellen oder immateriellen Schadens ist erforderlich (der bloße Verstoß von DSGVO-Vorschriften ist nicht ausreichend).
2. Auch Bagatellschäden sind umfasst.
3. Die Ermittlung der konkreten Schadensersatzhöhe obliegt den nationalen Gerichten.

Ist der Diebstahl von personenbezogenen Daten ein Identitätsdiebstahl?

Nun wurde der EuGH erneut im Rahmen eines Vorabentscheidungsverfahrens (verb. Rs. C-182/22 und C-189/2) um Beantwortung verschiedener Fragen zur Auslegung des Schadensersatzes nach Art. 82 DSGVO gebeten. Es geht bei den durch das AG München vorgelegten Fragen um zwei weitgehend vergleichbare Klagen gegen das Unternehmen Scalable Capital GmbH („Scalable“). Die beiden Kläger haben bei einer von der Scalable betriebenen Trading-App ein Nutzerkonto angelegt und zur Identifizierung personenbezogene Daten wie Name, Geburtsdaten sowie digitale Kopien ihrer Personalausweise hinterlegt. Diese Daten konnten von unbekannten Straftätern gestohlen werden. Das AG München ist der Auffassung, dass den Klägern grundsätzlich ein

Schadensersatz nach Art. 82 DSGVO zusteht. Um die Höhe des zu gewährenden Schadensersatzanspruchs zu bestimmen, hat das AG München das Verfahren ausgesetzt und dem EuGH Fragen zur Auslegung von Art. 82 DSGVO vorgelegt.

In dem daraufhin eingeleiteten Vorabentscheidungsverfahren hat nun der Generalanwalt Anthony Collins in seinen Schlussanträgen vom 26. Oktober Stellung genommen. In der behandelten Frage wollte das AG München wissen, ob ein Identitätsdiebstahl i.S.d. Erwägungsgrund 75 DSGVO bereits vorliegt und einen Anspruch auf Schadensersatz begründet, wenn Straftäter über Daten verfügen, die den Betroffenen identifizieren oder ob dieser erst gegeben ist, wenn sich Straftäter bereits als die betroffene Person ausgegeben haben.

Auch ein immaterieller Schaden muss bewiesen sein

Der Generalanwalt betonte zunächst erneut, dass eindeutig und präzise bewiesen werden müsse, dass der Betroffene einen immateriellen Schaden erlitten habe. Ein bloß potenzieller oder hypothetischer Schaden oder die bloße Beunruhigung aufgrund des Diebstahls der eigenen personenbezogenen Daten stellen keinen ausreichenden Beweis dar. Ein immaterieller Schaden kann etwa vorliegen, wenn eine Person daran gehindert wird, ihre personenbezogenen Daten zu kontrollieren bzw. die Kontrolle über diese verliert.

Identitätsdiebstahl setzt Identitätsnutzung voraus

Die Begriffe Identitätsdiebstahl und Identitätsbetrug würden in der DSGVO erwähnt, jedoch nicht definiert. Aufgrund der Erwägungsgründe 75 und 85 DSGVO werde aber deutlich, dass der Diebstahl personenbezogener Daten selbst dann noch keinen Identitätsdiebstahl darstelle, wenn der Diebstahl dazu geeignet ist, die Grundlage dafür zu schaffen, dass diese Daten künftig (missbräuchlich) verwendet werden. Für die Annahme eines Identitätsdiebstahls sei zum Diebstahl der personenbezogenen Daten erforderlich, dass eine zusätzliche Handlung bzw. ein zusätzlicher Schritt mit nachteiligen Auswirkungen auf die betroffene Person gegeben ist. Beispielhaft müsse der Dieb etwa die Daten zu rechtswidrigen Zwecken verwenden oder zumindest konkrete Schritte diesbezüglich unternehmen. Letzteres Stadium ist den

Juristen unter uns vergleichbar noch aus dem Strafrecht bekannt, wenn es um die Bestimmung des „Versuchs“ ging.

So sei zwar der Diebstahl personenbezogener Daten allein noch kein Identitätsdiebstahl bzw. Identitätsbetrug. Allerdings könne der Diebstahl dennoch bereits zu einem Anspruch auf immateriellen Schadensersatz führen. Dieser müsse aber bewiesen werden.

Folgen für die Praxis

Die rechtliche Würdigung des Generalanwalts führt die Wertungen des EuGH zum immateriellen Schadensersatz fort: Es ist stets der Nachweis eines konkret erlittenen immateriellen Schadens erforderlich, um einen Schadensersatzanspruch nach Art. 82 DSGVO zu begründen. Dieser Nachweis kann womöglich einfacher zu erbringen sein, wenn die betroffene Person tatsächlich Opfer eines Identitätsdiebstahls geworden ist – aber auch der bloße Diebstahl personenbezogener Daten an sich kann einen immateriellen Schadensersatzanspruch begründen. Die „Vollendung“ eines Identitätsdiebstahls ist in solchen Fällen also keine zwingende Voraussetzung für den Schadensersatzanspruch der Opfer. Abzustellen ist – wie immer – auf die konkreten Umstände des Einzelfalls.

EuGH: Was sind personenbezogene Daten?

Der EuGH hat in einer aktuellen Entscheidung konkretisiert, wann Nummernfolgen personenbezogene Daten sind. Konkret ging es um die FIN als eindeutige Identifikationsnummer von Fahrzeugen, die Urteilsgründe können auch auf andere IDs und Kennziffern, etwa die dynamische IP-Adresse, übertragen werden. Für die Praxis ist die Entscheidung von elementarer Bedeutung.

Die FIN kennzeichnet ein Fahrzeug. Für den Fahrzeughersteller hat sie zunächst keinen Bezug zu einer natürlichen Person. Dies kann sich aber ändern, wenn das Fahrzeug auf eine natürliche Person zugelassen wird oder eine natürliche Person in der Zulassungsbescheinigung als Fahrzeughalter gelistet ist. Dann nämlich kann die FIN (= Fahrzeug-Identifizierungsnummer) mithilfe der weiteren Angaben in der Zulassungsbescheinigung einer natürlichen Person – dem Inhaber der Zulassung oder der Fahrzeughalterin – zugeordnet werden.

Das Verfahren

Der EuGH hatte nun in einem in Köln gestarteten Verfahren zu entscheiden, ob und wann die FIN ein personenbezogenes Datum i.S.d. Art. 4 Nr. 1 DSGVO ist. Der Entscheidung liegt ein Vorabentscheidungsersuchen aus Köln zugrunde (Urteil vom 09.11.2023 – C-319/22 – Scania). Der Gesamtverband Autoteile-Handel e.V: verlangte von Scania umfassendere Informationen bei Nachfrage nach der FIN, da dies verordnungsrechtlich geboten sei. Scania hielt dem Grenzen des Datenschutzes entgegen.

Das LG Köln legte daraufhin dem EuGH u.a. zur Vorabentscheidung vor, ob sich aus der EU-Verordnung über die Marktüberwachung von Kraftfahrzeugen eine rechtliche Pflicht i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO zur Herausgabe der FIN und mit ihr verknüpften Informationen ergebe.

Diese Frage ist nur dann erheblich, wenn diese Informationen personenbezogene Daten darstellen. Der EuGH prüfte denn auch dieses Element im ersten Schritt. Erst danach widmete er sich der Auslegung der „rechtlichen Pflicht“ nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO.

IDs als personenbezogene Daten

Für die Praxis höchst relevant auch über die FIN hinaus – etwa für dynamische IP-Adressen oder andere Kennungen – ist die zunächst behandelte Frage, ob und wann die FIN ein personenbezogenes Datum i.S.d. DSGVO darstellt. Der EuGH prüft dies lehrbuchhaft und im Detail sehr hilfreich.

Entscheidend ist:

- Kann die Nummer – hier die FIN – zu einer natürlichen Person führen?
- Verfügt derjenige, der die Nummer erhält, „bei vernünftiger Betrachtung über Mittel […], die es ermöglichen, sie einer bestimmten Person zuzuordnen"?

Erste zentrale Erkenntnis und Bestätigung aus dieser Entscheidung: Der Personenbezug ist für die Rechtseinheit zu prüfen, die die Nummer verarbeitet. Der EuGH bestätigt damit den relativen Ansatz: Die FIN kann für Unternehmen A ein personenbezogenes Datum darstellen, da sie über zusätzliche Informationen verfügen, diese einer natürlichen Fahrzeughalterin zuzuordnen, für Unternehmen B dagegen nicht.

Zweite zentrale Erkenntnis: Bei der Prüfung sind nicht alle theoretisch denkbaren Mittel, sondern nur die bei vernünftiger Betrachtung auch wirklich verfügbaren Mittel einzubeziehen. Dies ergibt sich auch aus Erwägungsgrund 26 DSGVO.

Datenverarbeitung zur Erfüllung rechtlicher Pflichten

Eine für die Praxis ebenfalls wesentliche Konkretisierung gibt der EuGH zur Verarbeitungserlaubnis „rechtliche Pflichten" i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO.

Will sich ein Verantwortlicher auf diese Erlaubnisgrundlage stützen, so ist präzise zu prüfen

- ob die Verarbeitung auch der personenbezogenen Daten für die Erfüllung der rechtlichen Pflicht tatsächlich erforderlich ist und
- ob diese Verarbeitung in einem angemessenen Verhältnis zum verfolgten, legitimen Zweck steht.

Konkret bedeutet dies (**dritte zentrale Erkenntnis**): Die Erfüllung einer rechtlichen Pflicht reicht nicht, auch in der Abwägung muss die Verarbeitung angemessen erscheinen. Ist dies nicht der Fall, „überwiegt" das datenschutzrechtliche Verbot und eine Verarbeitung ist datenschutzrechtlich trotz rechtlicher Pflicht nicht erlaubt. Dies ergibt sich aus Art. 6 Abs. 3 DSGVO. Die EuGH-Entscheidung zeigt allerdings deutlich, welche Prüf- und Bewertungslast hier auf den Schultern der Verantwortlichen ruht.

Zu guter Letzt

Anstelle der üblichen Bußgeldentscheidungen gibt es in dieser Ausgabe deutlich spannendere Vorgänge im Datenschutzbereich: Der BSI-Lagebericht 2023 offenbart eine weiter angespannte Lage in Sachen Cyber-Sicherheit. Dies bestätigt sich denn auch in aktuellen Datenlecks, etwa bei Microsoft, Sony und 23andMe. Und auch in Sachen personalisierter Werbung und Tracking gibt es neue Entwicklungen: Google wurde zur Zahlung von 93 Millionen US-Dollar wegen heimlichen Trackings verpflichtet und bei Meta soll personalisierte Werbung verboten werden.

- **BSI-Lagebericht zur IT-Sicherheit in Deutschland**

Am 2. November hat das BSI seinen jährlichen Lagebericht zur IT-Sicherheit in Deutschland veröffentlicht. Die Lage ist nach wie vor angespannt. Das BSI titelt gar: „Die Bedrohung im Cyberraum ist so hoch wie nie zuvor". Zunehmend werden auch mittlere

Unternehmen Opfer von Cyber-Attacken, die Cyber-Kriminalität wird immer professioneller.

Ab dem nächsten Jahr wird der BSI-Lagebericht nochmals wichtiger: Alle von dem neuen IT-Sicherheitsrecht adressierten Unternehmen müssen diesen nach dem aktuellen Stand des Gesetzesentwurfs zur Umsetzung der NIS-2-Richtlinie bei ihren Risikomanagementmaßnahmen beachten. Wir empfehlen daher schon jetzt einen Marker im Kalender auf Ende Oktober/Anfang November zu legen und dann den neuen Lagebericht auszuwerten, um Nachjustierungen im eigenen Unternehmen in Sachen IT-Sicherheit einzuplanen.

- **Datenleck bei Microsoft: KI-Forscher veröffentlichen versehentlich 38 TB interne Daten**

Sicherheitsforscher des IT-Unternehmens Wiz haben das Internet auf der Suche nach irrtümlich veröffentlichten Datensätzen durchsucht – und dabei ein Datenleck bei Microsoft aufgedeckt. Die Forscher haben sich ein öffentliches GitHub-Repository (ein Webdienst zur kollaborativen Softwareentwicklung) eines KI-Forschungsteam von Microsoft angeschaut. Interessierten sollte es hier ermöglicht werden, Trainingsdaten herunterzuladen. Allerdings war es über die dort von Microsoft hinterlegte URL möglich, nicht nur auf die Trainingsdaten, sondern auf das gesamte Speicherkonto zuzugreifen. Auf diese Weise hat das KI-Forschungsteam von Microsoft versehentlich 38 Terabyte privater Daten offengelegt, die u.a. zum Trainieren von Künstlicher Intelligenz genutzt wurden. Zwei Tage nachdem Wiz Microsoft über das Datenleck informierte, schloss Microsoft den Zugang und leitete Untersuchungen über mögliche interne Auswirkungen ein. Diese ergaben eigenen Angaben zufolge, dass weder Kundendaten offengelegt noch andere interne Dienste gefährdet waren. Nach Ansicht von Wiz sei der Fall ein Beispiel für die neuen Risiken, mit denen Unternehmen konfrontiert sind, wenn sie die Möglichkeiten der KI in größerem Umfang nutzen, da immer mehr ihrer Ingenieure mit großen Mengen von Trainingsdaten arbeiten. Diese riesigen Datenmengen erfordern daher zusätzliche Sicherheitsüberprüfungen und Schutzmaßnahmen.

- **Polen: Untersuchungen der Datenschutzbehörde gegen ChatGPT**

Letzten Monat wurde in Polen eine Beschwerde gegen OpenAI und ihren KI-Chatbot ChatGPT eingereicht, in der dem Unternehmen verschiedene Verstöße gegen die DSGVO vorgeworfen wurden. ChatGPT wird u.a. zur Last gelegt, unrichtige Informationen des Beschwerdeführers zu verarbeiten und seinen Informationsrechten nach Art. 12 DSGVO nicht ausreichend nachgekommen zu sein – beispielsweise habe ChatGPT ihm keine Auskunft darüber geben können, welche Daten des Beschwerdeführers verarbeitetet werden.

Inzwischen hat das polnische Amt für den Schutz personenbezogener Daten (UIDO) eine Untersuchung hierzu eingeleitet. Eine Herausforderung wird insbesondere darin gesehen, dass ChatGPT ihren Sitz in San Francisco, also außerhalb der EU hat. Dies ist nicht das erste Mal, dass eine Datenschutzbehörde eines Mitgliedsstaats datenschutzrechtliche Bedenken hinsichtlich des ChatBots hat. Die italienische Datenschutzbehörde etwa hatte diesen wegen Datenschutzbedenken gesperrt – siehe hierzu den obigen Beitrag und unseren Newsletter aus April 2023. Der Europäische Datenschutzausschuss (EDSA) hat daher mittlerweile eine Arbeitsgruppe für die Bewertung von ChatGPT eingerichtet.

- **Kalifornien: Google zahlt 93 Millionen US-Dollar wegen heimlichem Tracking**

Der Generalstaatsanwalt des US-Bundesstaates Kalifornien hat den Konzern Google mit Sitz in Mountain View (Kalifornien) beschuldigt, seine Nutzer im Hinblick auf die Verarbeitung ihrer Standortdaten getäuscht zu haben. So habe Google beispielsweise auch diejenigen Nutzer gezielt getrackt, die die Standort-Verfolgung deaktiviert haben. Auf diese Weise ließe Google seine Nutzer in dem Glauben, diese könnten bestimmen, welche Daten Google erhebt. Dies stelle einen Verstoß gegen kalifornische Verbraucherschutzrechte dar. Mittlerweile haben Google und der US-Bundesstaat einen Vergleich darüber geschlossen, nach dem Google 93 Millionen US-Dollar an den Bundesstaat zahlen und seinen Datenschutz in vielerlei Hinsicht verbessern soll.

- **Verbot der personalisierten Werbung auf Instagram und Facebook?**

Was in Norwegen bereits seit einigen Wochen gilt, soll zeitnah in der ganzen EU verwirklicht werden: Ein Verbot verhaltensbasierter, personalisierter Werbung auf den Meta-Plattformen Instagram und Facebook. Hintergrund ist eine Positionierung von Meta, die auch in kartellrechtlichen Verfahren schon für Gegenwehr gesorgt hat: Der Abschluss des Nutzungsvertrages sieht die Schaltung personalisierter Werbung vor, bisweilen als „Vorteil der Nutzer" deklariert, da diese nur für sie wirklich interessante Werbung sähen.

Diese Auslegung der Erlaubnisgrundlage in Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO (Vertragserfüllung) steht schon länger in der Kritik. Es fehle u.a. an der transparenten Darstellung, echten Wahlmöglichkeiten und letztlich der Erforderlichkeit für die Leistungserbringung. Gegen das in Norwegen schon geltende Verbot ist Meta im einstweiligen Rechtsschutz erfolglos vorgegangen, es gilt weiter. Nun soll die gesamte EU nachziehen, durch eine Entscheidung der für Meta zuständigen irischen Datenschutzaufsichtsbehörde.

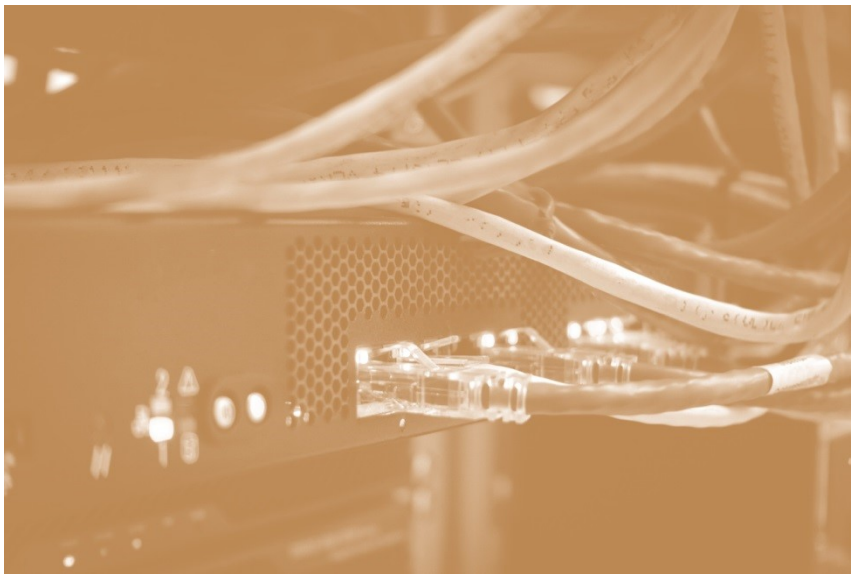
Meta hat denn auch schon angekündigt, auf ein Einwilligungsmodell umzusteigen. Der Meta-Konzern bietet Nutzern in der Europäischen Union zukünftig Versionen ohne Werbung, dafür gegen Bezahlung an. Der Konzern erhofft sich hierdurch, sich zukünftig weniger angreifbar in Sachen Datenschutz zu machen. Der Roll-Out ist in vollem Gang: 12,99 Euro monatlich soll die Variante ohne Werbe-Tracking auf mobilen Endgeräten kosten, 9,99 Euro im Webbrowser. Die Mobilversion sei deshalb teurer, da Apple und Google auch Gebühren erheben würden, die an die Kunden so weitergegeben werden sollen. Solange Nutzer die Bezahlversion beziehen, sollen ihre Informationen nicht genutzt werden für Werbung. Hintergrund der Einführung sei, dass Meta so weiterhin seine Dienste in der EU/den EWR-Staaten sowie der Schweiz anbieten könne ohne gegen die DSGVO zu verstoßen.

Umgesetzt wird damit ein Konstrukt, das aus der Medienlandschaft bekannt und dort auch von den Datenschutzaufsichtsbehörden dem Grund nach gebilligt ist (zu Recht, müssen sich doch gerade die Zeitschriftenverlage digital refinanzieren können, um auch künftig eine Mediendemokratie zu ermöglichen). Aber passt das als „PUR-Modell" bekannte System auch für die Social Media-Plattformen von

Meta? Und sind Kosten in Höhe von ca. 13 bzw. 10 Euro noch so erschwinglich (auch mit Blick auf die Nutzergruppe), dass dies eine freiwillige Entscheidung für das Werbetracking ermöglicht? Dies sollte diskutiert werden und auch, ob die Informationen so transparent erfolgen, dass der Durchschnittsnutzer seine Entscheidung auch versteht…

- **Hacker bieten geklaute Datensätze vom Genetik-Testunternehmen „23andMe“ zum Verkauf an**

Das im April 2006 gegründete und durch Google mitfinanzierte US-Unternehmen „23andMe“ bietet Privatpersonen an, mithilfe einer Speichelprobe, ihre genetischen Informationen u.a. auf die Wahrscheinlichkeit des Auftretens von zukünftigen Krankheiten zu untersuchen. Eine Besonderheit von genetischen Datensätzen ist, dass diese nicht nur Informationen der Kunden, die diese bereitgestellt haben, umfassen – sondern darüber hinaus Informationen über Unbeteiligte, die Teile des genetischen Codes teilen. Bereits im Jahr 2008 warnten Datenschützer davor, dass die sensiblen Daten gehackt werden könnten. Nun ist diese Befürchtung wahr geworden – Hacker haben mehrere Millionen Datensätze von 23andMe gestohlen. Hierüber hat das Unternehmen ihre Kunden per E-Mail informiert. Die Datensätze umfassen Namen, Profilbilder, Geburtsdaten sowie Ergebnisse der Genanalyse der Kunden. Es ist bisher unklar, wie viele Kunden genau betroffen sind.



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

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Dennis Pethke, LL.M.
+49(0)221 65065-337
dennis.pethke@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