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

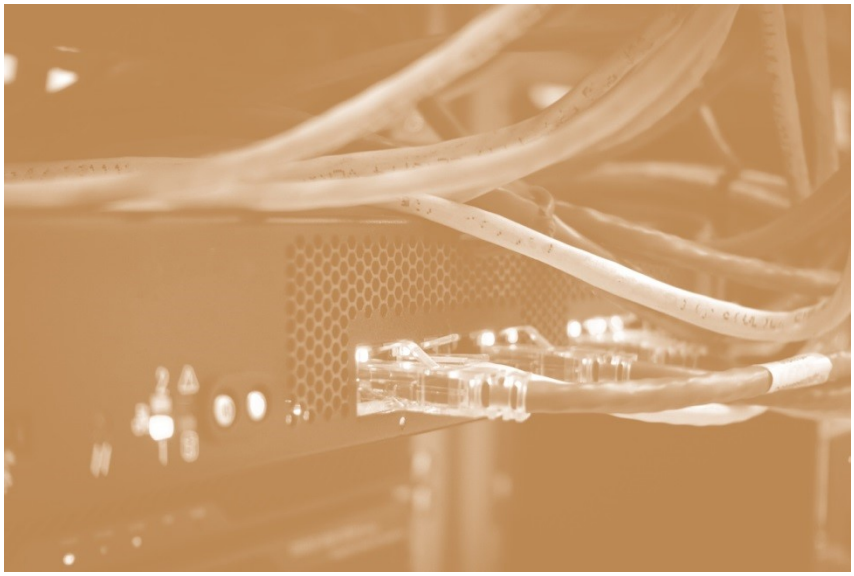
Union zukünftig Versionen ohne Werbung, dafür gegen Bezahlung an. Der Konzern erhofft sich hierdurch, sich zukünftig weniger angreifbar in Sachen Datenschutz zu machen. Der Roll-Out ist in vollem Gang: 12,99 Euro monatlich soll die Variante ohne Werbe-Tracking auf mobilen Endgeräten kosten, 9,99 Euro 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 65065-200
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