LOSCHELDER

Newsletter Datenschutzrecht

April 2023

Sehr geehrte Damen und Herren,

die österliche Entspannung der letzten Tage wird es erträglicher machen, erneut in die Herausforderungen des DSGVO-konformen Drittstaatentransfers von Daten abzutauchen. Wir bringen hierzu einige Hilfestellungen in unseren Beiträgen 1 bis 3!

Hoch interessant ist das Ansinnen, die Durchsetzung der DSGVO zu vereinheitlichen – wir berichten Ihnen darüber in unserem 4. Beitrag.

Zu guter Letzt gibt es wieder einige interessante Behörden- und Gerichtsentscheidungen in diesem Monat. Zum Beispiel wurde einem Kläger Schadensersatz in Höhe von 10.000 Euro wegen unzureichender Auskunft zugesprochen und in Italien wurde die Künstliche Intelligenz ChatGPT durch die italienische Datenschutzbehörde gesperrt.

Wir freuen uns über Ihr Interesse!

Inhalt

Neues zum Drittstaatentransfer?

Die meisten großen Tech-Giganten sind in den USA ansässig. Die Nutzung der Dienste von Apple, Microsoft, Google & Co. ist für Unternehmen oftmals alternativlos. Da die USA ein Drittland im Sinne der DSGVO sind, muss der Datentransfer dorthin spezifisch abgesichert sein. Seit dem EuGH-Urteil in Sachen Schrems II ist das kein einfaches Unterfangen. Nun zeichnet sich eine Lösung in Form eines neuen Angemessenheitsbeschlusses ab.

Unternehmen müssen für den Einsatz von Drittanbietern, die personenbezogene Daten in die USA transferieren, die Absicherung dieses Transfers nach den Vorgaben der Art. 44 ff. DSGVO sicherstellen. Dies erfordert nach dem Schrems II Urteil des EuGH ein „Transfer Impact Assessment", eine Risikobewertung, ob die gewählten Maßnahmen zu einem hinreichenden Sicherheitsniveau führen. Dies führt in der Praxis regelmäßig zu ganz erheblichen Herausforderungen. Neue Entwicklungen sind dabei stets im Blick zu halten. Wir haben Ihnen einige wesentliche Neuerungen zusammengefasst:

Beschluss der DSK zu Drittlandtransfers

Erwähnenswert ist zunächst der Beschluss der Datenschutzkonferenz (DSK) vom 31. Januar 2023 zur Bewertung von Zugriffsmöglichkeiten von Drittland-Behörden auf personenbezogene Daten. Genau diese Zugriffsmöglichkeit von Sicherheitsbehörden in den USA war ein entscheidender Grund für den EuGH, die Sicherheit personenbezogener Daten in den USA anzuzweifeln.

Gem. Art. 44 ff. DSGVO ist eine Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation nur unter bestimmten Bedingungen zulässig: Im Drittland muss ein angemessenes Datenschutzniveau gesichert sein. Dies beinhaltet auch, dass Zugriffe von Sicherheitsbehörden nur entsprechend der EU-Standards zulässig sein dürfen, also u.a. nur in verhältnismäßigem Umfang und mit effektiven Rechtsmitteln gegen einen solchen Zugriff.

Aber wann liegt überhaupt eine „Übermittlung" vor, für die die Art. 44 ff. DSGVO zu beachten sind? Die DSK hält dazu jetzt fest, dass nicht bereits die bloße Gefahr eines Zugriffs auf Daten aus den USA heraus

eine Drittlandübermittlung sei. Dies ist folgerichtig, da nach der DSGVO-Beschreibung der Übermittlung in Art. 44 ff. und den zugehörigen Erwägungsgründen eben der Zugriff als solcher entscheidend ist, nicht aber eine (abstrakte) Gefahr. Aber hilft eine solche Aussage in der Praxis?

Eher nicht: Zum einen muss ich als Unternehmen einen operativ handhabbaren Modus finden. Tools können nicht spontan ausgetauscht werden, wenn sich eine solche Gefahr einmal konkretisieren oder realisieren sollte. Zum anderen relativiert die DSK ihre Aussage auch selbst: Die abstrakte Gefahr eines Datenzugriffs könne dazu führen, dass beim Einsatz als Auftragsverarbeiter die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt. Dies gelte auch für die EU-Töchter von US-Unternehmen, wenn eben aufgrund der US-Regeln das Risiko besteht, dass die Töchter über die US-Mütter zur Datenherausgabe gezwungen werden könnten.

Damit geht es „zurück auf Los“: Die DSK hält den Einsatz der US-Tools, auch bei EU-Tochterunternehmen als Anbietern, im Ergebnis für kritisch. Dies hilft in der Praxis nicht.

Richtlinie des Europäischen Datenschutzausschusses (EDSA)

Neu gefasst sind weiter die Leitlinien des EDSA, in denen der Begriff des Drittstaatentransfers konkretisiert wird (Guidelines 05/2021, jetzt in der Version 2.0 vom 14.02.2023). Revolutionäre, neue Erkenntnisse ergeben sich aus diesen also nicht. Auch hieraus ergibt sich für die Praxis daher wenig Hilfestellung.

EU-US Datenabkommen 3.0

Eine echte rechtssichere Erleichterung könnte dagegen ein neuer Angemessenheitsbeschluss für die USA bringen: Das EU-US Datenabkommen 3.0 bietet hierfür die Grundlage. Der Entwurf der Kommission für den Angemessenheitsbeschluss liegt bereits seit einiger Zeit vor.

Nach ursprünglicher Kritik an dem Entwurf begrüßt der EDSA inzwischen getroffene Anpassungen, auch wenn wesentliche Kritikpunkte bleiben.

Dennoch: Die Zeichen stehen auf „grün“, es wird erwartet, dass der Angemessenheitsbeschluss im Laufe dieses Jahres erlassen wird.

Optimisten erwarten dies schon im Sommer, realistischer ist der Erlass im Herbst 2023. Ist der Angemessenheitsbeschluss wirksam, bringt das eine echte Hilfe in der Praxis. Auch wenn NOYB und der Aktivist Max Schrems ihre Ankündigung wahrmachen sollten und erneut vor den EuGH ziehen, bleibt der Angemessenheitsbeschluss wirksame Grundlage für Datentransfers in die USA, bis der EuGH ihn – sollte dies erneut der Fall sein – für unwirksam erklärt.

Die Evergreens: Google Analytics und Facebook

Google Analytics und Facebook sind wohl die am häufigsten genutzten Tools im Unternehmensmarketing. Daher und zugleich sind Google Analytics und Facebook wohl auch die von den Datenschutzaufsichtsbehörden am schärfsten kritisierten Anwendungen. Zu beiden Angeboten gibt es neue Entwicklungen – eine neue Version von Google Analytics und ein erwarteter Rechtsstreit, der die Zulässigkeit von Unternehmensseiten auf Facebook klären könnte.

Das neue Google Analytics 4

Google Analytics ist ein Analysetool des US-amerikanischen Unternehmens Google LLC. Mit ihm können Websitebetreiber analysieren, welche Gruppen welche der Unterseiten wie lange besuchen, wo die Nutzer abspringen, was besonders interessiert u.v.m.. Möglich ist auch eine Analyse über Seiten und Endgeräte hinweg, die Erfolgsmessung von Kampagnen und etliches mehr. Erfasst werden u.a. die Herkunft der Webseitenbesucher, ihre

Verweildauer sowie die Nutzung von Suchmaschinen. Deaktiviert der Websitebetreiber die Funktionen nicht, verfolgt Google den Nutzer mit einer eindeutigen Kennung, die eine Wiedererkennung möglich macht. Die Datenschutzaufsichtsbehörden haben am Einsatz u.a. genau dies kritisiert und auch die Verwendung der Analysedaten durch Google zu eigenen Zwecken beanstandet.

Fallen die Bedenken mit der neuen Version Google Analytics 4 nun weg?

Durch die neue Version Google Analytics 4 (GA4) verspricht Google eine verbesserte Datenschutzkonformität. Beispielsweise sollen Daten aus der EU auch ausschließlich in der EU gespeichert und verarbeitet werden, die Daten seien größtenteils zudem verschlüsselt.

Die Aufsichtsbehörden teilen diese Einschätzung nicht: Die österreichische, französische und die italienische Datenschutzaufsichtsbehörde sehen auch in der neuen Version von Google Analytics Verstöße gegen die DSGVO. Es sei insbesondere immer noch nicht sichergestellt, dass US-amerikanische Sicherheitsbehörden nicht auf personenbezogene Daten zugriffen.

Anders als ursprünglich erhofft, arbeitet zudem auch GA4 weiterhin mit Cookies. Es bleibt damit beim Einwilligungserfordernis nach aktuellem Diskussionsstand. Auch in diesem Aspekt bleiben damit letztlich die bekannten Risiken und Herausforderungen bestehen. Kurzum: GA4 ist aus Marketingsicht womöglich ein Fortschritt, in Sachen DSGVO bleibt es dagegen bei den altbekannten Risiken.

Untersagung des Betriebs der Facebook-Fanpage der Bundesregierung

Mit einem Paukenschlag hat das BfDI vor kurzem dem Presseamt der Bundesregierung den Betrieb deren Facebook-Fanpage untersagt.

Damit ist wahr geworden, was die Datenschutzaufsichtsbehörden seit langem ankündigen: Sie würden, so heißt es seit Monaten, gegen den Betrieb von Fanpages auf Facebook vorgehen. Denn dieser sei datenschutzrechtlich nicht zulässig gestaltbar. Auch hieß es seit langem, erst seien die öffentlichen Stellen „an der Reihe“. Für die Risikobetrachtung bedeutete dies: Solange die Aufsichtsbehörden nicht gegen öffentliche Stellen vorgehen, haben auch private Unternehmen wohl nichts zu befürchten.

Damit ist es jetzt vorbei. Die erste Facebook-Fanpage wurde untersagt. Getroffen hat es die Seite des Bundespresseamtes – ein strategisch und medial höchst wirkungsvoller Schritt des BfDI.

Als Antwort darauf hat das Presseamt der Bundesregierung inzwischen bekannt gegeben, an der Facebook-Fanpage festhalten zu wollen. *Sie sei ein wichtiger Bestandteil der Öffentlichkeitsarbeit, um Informationen mit der Bevölkerung zu teilen und dabei insbesondere Desinformation entgegenzutreten*. Das Presseamt kündigte an, notfalls auch gegen den Bescheid des BfDI vorzugehen. Kommt es dazu, könnte in dieser praktisch so höchst relevanten Frage endlich mehr Klarheit und Rechtssicherheit auch für die privaten Unternehmen erreicht werden.

Maßnahmen für den datenschutzgerechten Einsatz von Microsoft 365

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat im November 2022 bereits zum zweiten Mal infrage gestellt, dass Microsoft 365 datenschutzkonform eingesetzt werden kann. Die eigentlich logische Konsequenz, den Einsatz zu verbieten, ziehen die Datenschutzbehörden allerdings nicht. Verantwortliche sind durch dieses Verhalten der Aufsichtsbehörden ein Stück weit auf sich gestellt und sollten im Rahmen einer Selbsteinschätzung über den Einsatz entscheiden. Nachfolgend stellen wir daher Maßnahmen vor, mit denen das Risiko des Einsatzes zumindest reduziert werden kann – gerade auch mit Blick auf das neue Angebot von Microsoft (EU Data Boundaries).

Das zentrale Problem beim Einsatz von Microsoft 365 (MS 365) ist, dass es sich bei den Programmen um komplexe Anwendungen handelt, in denen auf unterschiedliche Weise und von unterschiedlichen Akteuren Daten verarbeitet werden. Da es sich bei der Microsoft Gruppe um einen internationalen Konzern handelt, finden die Verarbeitungen zudem teilweise in Drittstaaten statt und potentiell in allen Ländern, in denen Microsoft tätig wird. Noch unübersichtlicher werden die Datenverarbeitungen dadurch, dass man als Kunde die Möglichkeit hat, innerhalb der MS 365-Anwendungen zahlreiche Tools von Drittanbietern zu verwenden, die wiederum Daten der Nutzer verarbeiten. Solche komplexen Anwendungen sind mit den Vorgaben des Datenschutzrechts schwer in Einklang zu bringen.

Problemübersicht

Datenschutzrechtlich problematisch sind insbesondere die folgenden Punkte:

- **Auftragsverarbeitungsvertrag**
  Für die Verwendung von MS 365 schließen der Kunde und die Microsoft Ireland Operations Limited (Microsoft) einen Auftragsverarbeitungsvertrag, den sogenannten „Datenschutznachtrag zu den Produkten und Services von Microsoft“ (DPA) ab. Das DPA wird fortlaufend überarbeitet und erneuert. Die aktuellste Version datiert vom 01.01.2023 (Stand: 14.04.2023) und enthält einige Punkte, die insbesondere von der DSK kritisiert werden, nämlich:

- **Rechenschaftspflicht**
  Microsoft ermächtigt sich in dem DPA zur Verarbeitung sogenannter (ggf. personenbezogener) Telemetrie- und Diagnosedaten für eigene Zwecke in eigener Verantwortung. Telemetrie- und Diagnosedaten sind Metadaten, die bei der Verwendung von MS 365-Produkten generiert werden. Es ist nicht hinreichend eindeutig, welche Daten Microsoft dabei für eigene Zwecke verarbeitet. Die Verantwortlichen können daher ihre Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nur unzureichend erfüllen.

- **Offenlegung von Daten**
  Microsoft behält sich die Offenlegungen von Daten gegenüber Behörden in Drittstaaten vor, falls Microsoft gesetzlich dazu gezwungen ist; dies widerspricht Art. 28 Abs. 3 S. 2 lit. a) DSGVO, der Datenverarbeitungen außerhalb der Weisungen des Verantwortlichen nur erlaubt, wenn das Recht der Union oder der Mitgliedstaaten die Verarbeitung vorschreibt.

- **Drittstaatentransfers**
  Microsoft behält sich vor, Daten aufgrund der Standardvertragsklauseln vom 04.06.2021 in alle Länder der Welt zu übermitteln, in denen Microsoft oder seine Unterauftragsverarbeiter tätig sind. Das ist eine große Zahl von Ländern, zu denen u.a. China, Indien, Marokko und andere Staaten gehören, in denen möglicherweise unverhältnismäßige Eingriffe in personenbezogene Daten vorgenommen werden können.

- **Rollenverteilung**
  Damit enthält bereits das von Microsoft verwendete DPA problematische Regelungen. Zusätzlich können bei der Anwendung von MS 365 Datenverarbeitungen erfolgen, die im DPA gar nicht erwähnt sind. So können aus MS 365-Anwendungen heraus bspw. Suchaktionen mit Microsoft Bing durchgeführt werden. Dabei ist Microsoft Verantwortlicher für die Datenverarbeitung, nicht der Kunde. Im DPA ist dies nicht aufgeführt. Ebenso wenig genannt werden Datenverarbeitungen in der Verantwortlichkeit von Drittanbietern, die bspw. bei der Nutzung von Teams eingebunden werden können.

- **Überwachung/Profiling**
  Untersuchungen haben zudem ergeben, dass mithilfe von Telemetrie- und Diagnosedaten die Aktionen von Nutzern teilweise lückenlos nachvollzogen werden können. Es bestehen keine Anzeichen dafür, dass Microsoft von dieser Möglichkeit Gebrauch macht. Dennoch begründet sie ein hohes Risiko für die Persönlichkeitsrechte der Nutzer.

- **Überwachung von Mitarbeitern**
  Einige Funktionen (Viva Insights, Teams Analytics, ggf. auch der Diagnostic Data Viewer, Statusanzeige in Teams) ermöglichen bei entsprechender Verwendungsabsicht eine übermäßige Kontrolle von Arbeitnehmern, die MS 365-Anwendungen verwenden.

Diese und weitere Datenverarbeitungen machen die Verwendung von MS 365 problematisch. Verantwortliche stehen den Problemen allerdings nicht machtlos gegenüber. Durch eine datenschutzfreundliche Konfiguration der MS 365-Anwendungen und ggf. der IT-Umgebung können die Risiken reduziert werden.

Erforderliche Konfigurationen/Maßnahmen zur sicheren Verwendung von Microsoft

Nachfolgend benennen wir Maßnahmen, mit denen die Risiken des Einsatzes von MS 365 begrenzt werden können. Welche der Maßnahmen im Einzelfall erforderlich sind, hängt auch davon ab, welche Art von Daten ein Verantwortlicher in welchem Umfang verarbeitet. Eine Kindertagesstätte, in der sensible Daten von Kindern verarbeitet werden, muss sicherlich intensivere Maßnahmen ergreifen als bspw. ein Handelsunternehmen, das mit geschäftlichen Kontaktdaten von Ansprechpartnern arbeitet.

- **Auftragsverarbeitungsvertrag**
  Was zunächst die vertraglichen Mängel des DPA angeht, haben die meisten Kunden wohl nur sehr geringe Einwirkungsmöglichkeiten. Bei sehr großen, verhandlungsstarken Partnern von Microsoft kann es gelegentlich und im Ausnahmefall zu individuellen Vertragsanpassungen kommen. Den meisten Unternehmen wird aber regelmäßig nichts anderes übrigbleiben, als die Bedingungen zu akzeptieren. In diesem Fall bleiben den Verantwortlichen die folgenden Maßnahmen:

- **Aktualisierung:** Unternehmen sollten zunächst darauf achten, dass immer das aktuellste von Microsoft zur Verfügung gestellte DPA Anwendung findet. Hierfür müssen Verantwortliche die Geltung der DPAs gesondert mit Microsoft oder ihrem Microsoft Partner vereinbaren. Ansonsten gilt das DPA, das im Zeitpunkt der letzten vertraglichen Änderung galt.

- **Drittstaatentransfers:** Drittstaatenübermittlungen können teilweise durch die Verwendung der sogenannten EU Data Boundaries eingeschränkt werden. Bisher gilt das aber nicht für Telemetrie- und Diagnosedaten und für Professional Service Daten. Trotzdem führen die EU Data Boundaries schon jetzt zu einer erheblichen Risikominimierung. Voraussichtlich ab Anfang 2024 ist eine Nutzung von Microsoft vollständig ohne Datenübermittlungen in Drittstaaten möglich. Zusätzlich können sensible Daten durch eine Customer Lockbox verschlüsselt und so vor unbefugtem Zugriff gesichert werden.

- **Auftragsverarbeitungsvertrag:** Darüber hinaus bleibt den Verantwortlichen in Bezug auf etwaige Mängel des DPA, insbesondere im Hinblick auf die Einhaltung ihrer Rechenschaftspflicht, nur, diese zu analysieren und anschließend eine Risikoabwägung zu treffen.

- **Rollenverteilung**
  Die Verarbeitung von Daten durch Microsoft und etwaige Drittanbieter in eigener Verantwortung kann mithilfe der folgenden Maßnahmen und Konfigurationen eingeschränkt werden:

  - Deaktivieren der verbundenen Dienste und Erfahrungen
  - keine Integration von LinkedIn-Accounts der Nutzer
  - keine Datenübermittlung zur Verbesserung der Benutzerfreundlichkeit
  - Verbot von Drittanbieter Apps in Teams

- **Überwachung/Profiling**
  Eine unzulässige Ausforschung der Nutzer durch umfangreich erhobene Telemetrie- und Diagnosedaten kann mithilfe der folgenden Maßnahmen unterbunden werden:

  - Die Verwendung von **Telemetrie- und Diagnosedaten** durch Microsoft kann eingeschränkt werden, indem die Übermittlung hierfür auf „weder noch“ eingestellt wird. Zusätzlich kann die Übermittlung von Telemetriedaten auch mithilfe von technischen Maßnahmen eingeschränkt werden (Firewall), dies führt allerdings zu Funktionseinschränkungen bei der Verwendung von MS 365.

  - In mobilen Apps und Webversionen kann die Verarbeitung von **Telemetrie- und Diagnosedaten** durch Microsoft nicht eingeschränkt werden. Mobile Apps und Webversionen sollten daher nicht verwendet werden.

  - Welche Daten an Microsoft übermittelt werden, kann mithilfe des Diagnostic Data Viewers nachvollzogen werden.

- **Überwachung von Mitarbeitern**
  Die Verwendung von MS 365 darf nicht zu einer unzulässigen Ausforschung von Mitarbeitern führen. Dafür ist erforderlich:

  - keine Verwendung von Viva Insights, Teams Analytics, ggfs. auch der Statusanzeige bei Teams

  - kein Einsatz des Diagnostic Data Viewers, um Mitarbeiter unangemessen zu kontrollieren, dies kann durch interne Organisationsvorgaben, die dies untersagen, sichergestellt werden

  - Der Einsatz von MS 365 und die Verwendung zur Kontrolle von Mitarbeitern sollte mit dem Betriebsrat vereinbart und im Idealfall in einer Betriebsvereinbarung geregelt werden.

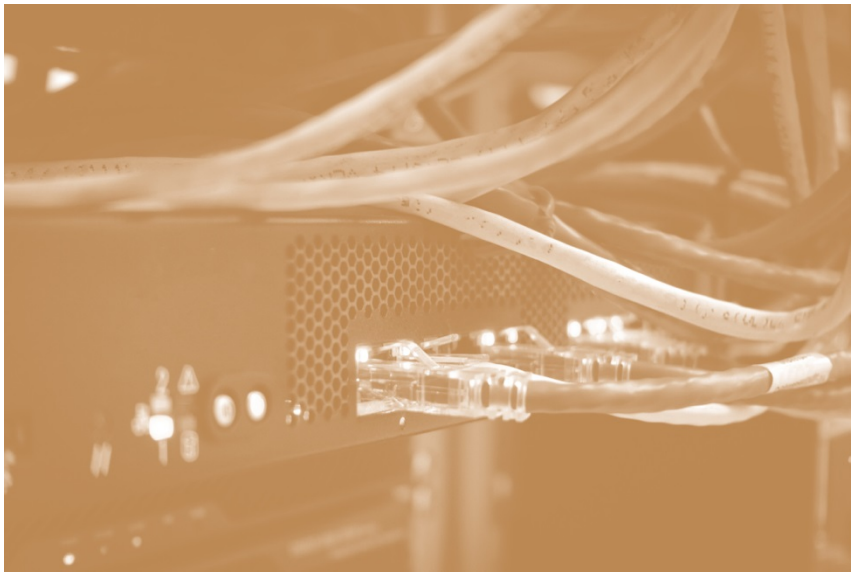
- **Sonstige Maßnahmen**
  Zusätzlich sollten E-Mails und 1:1-Telefonate per Teams verschlüsselt werden.

Datenschutz-Folgenabschätzung?

Verlässlich bewertet und zusätzlich abgesichert werden kann die Verwendung von MS 365, indem eine Datenschutz-Folgenabschätzung über die Verarbeitung von Daten mithilfe der Anwendungen durchgeführt wird. Ob dies rechtlich stets erforderlich ist, wird aktuell unterschiedlich bewertet. Nach einem jüngeren Urteil des LAG Rheinland-Pfalz vom 29.08.2022 (Az. 3 Sa 203/21, Rn. 61) begründet die Verarbeitung von Daten in einer MS 365-Cloud für sich genommen noch kein hohes Risiko für die Rechte und Freiheiten der Betroffenen. Eine Datenschutz-Folgenabschätzung ist demnach zumindest nicht bei allen Verantwortlichen obligatorisch. Je sensibler die Daten sind, die mithilfe der Anwendungen verarbeitet werden, desto eher ist aber eine Datenschutz-Folgenabschätzung erforderlich. Auch bei weniger sensiblen Daten kann sie helfen, die Risiken des Einsatzes von MS 365 korrekt einschätzen zu können.

Fazit

Der Einsatz von MS 365 birgt Risiken, die insbesondere mit den aufgeführten Maßnahmen reduziert werden können. Ein Restrisiko besteht daher auch bei einem kontrollierten Einsatz von MS 365. Über dieses Restrisiko muss eine informierte und bewusste Entscheidung getroffen werden.



Bessere Datenschutz-Durchsetzung durch DSGVO-Änderung?

Die DSGVO gilt einheitlich in der ganzen EU. Ihre Anwendung aber ist doch überaus unterschiedlich in den einzelnen Ländern. In der Kritik steht hier seit langem insbesondere die Handhabung in Irland: Dort sind die großen Tech-Unternehmen mit US-Müttern ansässig, allen voran Meta (Facebook). Aus Sicht vieler geht die irische Datenschutzaufsichtsbehörde indes nicht entschieden genug gegen Datenschutzverletzungen von Meta vor. Dies könnte sich durch eine Änderung der DSGVO nun ändern.

Die EU-Kommission hat zur vereinfachten Durchsetzung der DSGVO eine Gesetzesinitiative auf dem Weg gebracht, die Mitte des Jahres 2023 veröffentlicht werden soll. Sie soll sich auf das Verwaltungsverfahrensrecht der DSGVO beziehen. Zwar sind Details noch unklar, es wird jedoch vermutet, dass die EU-Kommission das „Irland-Problem" angehen möchte. In Irland sind nämlich die meisten europäischen Tochterunternehmen von US-amerikanischen Tech-Giganten wie Apple, Meta oder Google angesiedelt. Dementsprechend ist die irische Datenschutzbehörde DPC für die Überwachung dieser Unternehmen und insbesondere für die Verhängung von Bußgeldern diesen gegenüber gemäß Art. 55 Abs. 1 DSGVO zuständig.

Die DPC hat also nicht nur festzustellen, ob ein Verstoß gegen die DSGVO vorliegt, sondern bestimmt zudem die Höhe eines potentiellen Bußgeldes. So beklagen Datenschützer nicht zum ersten Mal eine Entscheidung der DPC, nach der Meta lediglich ein Bußgeld in Höhe von wenigen Millionen Euro zahlen musste, obwohl weitaus höhere Bußgelder angebracht seien. Nicht zu selten blieb die Behörde in der Vergangenheit bei Verdachtsfällen auf DSGVO-Verstöße untätig.

Durchsetzung der DSGVO durch die EDSA?

Als gemeinsames Gremium der europäischen Aufsichtsbehörden kommt es beim Europäischen Datenschutzausschuss (EDSA) häufig zu Entscheidungsvorlagen der DPC, bei denen diese meist überstimmt wird. Die EDSA hat dabei jedoch keine Durchsetzungsbefugnis in dem Sinne, als dass die DPC angewiesen werden könnte, ein bestimmtes Bußgeld zu verhängen. Die meisten der von der DPC bearbeiteten Fälle von EU-weiter Bedeutung sind

aktuell immer noch ungelöst. Teile der DSGVO müssten nun an die künftige Realität angepasst werden, forderte der EU-Datenschutzbeauftragte Wojciech Wiewiórowski.

Einen konkreten Entwurf zu den Änderungen gibt es noch nicht. Der EDSA äußerte allerdings einige „Wünsche“ für potentielle DSGVO-Änderungen. So soll beispielsweise eine Frist für bestimmte Verfahrensschritte bei der Bearbeitung von Fällen entstehen.

Zu guter Letzt

Auch in diesem Monat haben wir wieder spannende Entscheidungen für Sie zusammengefasst. In Italien ist ChatGPT untersagt worden. Die österreichische Datenschutzbehörde hat sich zur Nutzung von Facebook Pixeln auf Websites geäußert und erklärt diese wegen unzulässiger Datenübermittlung für rechtswidrig. Zudem gab es wieder ein beachtlich hohes Bußgeld für eine norwegische Fitnessstudio-Kette, wegen unbeantworteten Auskunftsersuchen und unzulässiger Datenverarbeitung.

- **Italien: ChatGPT wird aus Datenschutzgründen gesperrt.**

Die italienische Datenschutzaufsichtsbehörde hat Bedenken, ob beim Einsatz von ChatGPT dem Jugend- und Datenschutz ausreichend Rechnung getragen wird. Die Reaktion: ChatGPT wird in Italien gesperrt, der Anbieter OpenAI hat nun 20 Tage Zeit zur Nachbesserung. Anlass der Aktion war eine Datenpanne, Ende März war der Chatverlauf anderer aktiver Nutzer einsehbar. Dies ist

allerdings nicht der eigentliche Grund für die Maßnahmen; die dortige Behörde bemängelt vielmehr umfangreiche Datensammelaktivitäten ohne Rechtsgrundlage, die OpenAI zu Trainingszwecken verwende.

- **ArbG Oldenburg: 10.000 Euro Schadensersatz wegen unzureichender Auskunft**

Verstöße gegen Art. 15 DSGVO haben schon in verschiedenen Gerichtsverfahren zu Schadensersatzforderungen geführt. Diese waren aber regelmäßig gering. Eine deutlich höhere Summe sah jetzt das ArbG Oldenburg in einem Urteil vom 09.02.2023 (Az. 3 Ca 150/21) für gerechtfertigt an: Ganze 10.000 Euro wurden dem dortigen Kläger zugesprochen, 500 Euro für jeden Monat Verzögerung. Das verantwortliche Unternehmen war seiner Auskunftspflicht über 20 Monate nicht nachgekommen.

- **Österreich: Nutzung von Facebook-Trackingdienste**

Von Meta bereitgestellte Facebook Pixel werden unter anderem zur Nutzerverfolgung und Schaltung personalisierter Werbung auf Websites verwendet. Besucht ein Nutzer die Website vom Unternehmen A, kann – bei Aktivierung des Pixels – diesem Nutzer bei einem späteren Besuch auf Facebook oder Instagram gezielt Werbung für die Produkte von Unternehmen A angezeigt werden.

Möglich wird dies über eindeutige Kennungen und damit der Verarbeitung personenbezogener Daten. Nach Ansicht der Behörde in Österreich würden dabei indes auch persönliche Informationen der Websitenutzer an das US-Unternehmen sowie die NSA übersandt. Dies sei mit den DSGVO-Anforderungen an einen zulässigen Drittstaatentransfer unvereinbar, mit Meta abgeschlossenen Standardvertragsklauseln seien ohne zusätzliche Maßnahmen unzureichend. Erneut ist dieser Bescheid der Behörde in einem Beschwerdeverfahren der Aktivisten-Organisation von Max Schrems, NOYB, ergangen. Offen bleibt angesichts des in diesem Verfahren zugrundeliegenden Sachverhalts, ob eine wirksame Einwilligung möglich ist. Denn sicher ist: Ohne Einwilligung darf ein solcher Pixel in Deutschland schon wegen den Anforderungen des TTDSG nicht eingesetzt werden.

- **Norwegen: Das Fitnessunternehmen SATS ASA muss ein Bußgeld in Höhe von 900.000 Euro zahlen**

Im Zeitraum von 2018 bis 2021 erhielt die norwegische Datenschutzbehörde mehrere Beschwerden darüber, dass die Fitnesscenter-Kette Sats ASA einer Vielzahl von Betroffenenanfragen zum Recht auf Auskunft oder Löschung nicht nachgekommen war. Dies bestätigte sich in den Untersuchungen der Datenschutzbehörde. Zudem stellte die Behörde fest, dass Sats einige Daten über die Trainingshistorie von Kunden, ohne eine rechtliche Befugnis diesbezüglich, verarbeitet hatte.

Bei dem Unternehmen handelt es sich um eine Kette mit Fitnessstudios in allen Ländern Skandinaviens, welches einer der marktführenden Anbieter in dieser Branche ist. Aufgrund der Verstöße erhielt Sats ein Bußgeld von 900.000 Euro.

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

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