LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2022

Sehr geehrte Damen und Herren,

im Jahresendspurt bringt unser letzter Newsletter für das Jahr 2022 noch eine Reihe praktisch hoch relevanter Themen: Die Diskussion um Microsoft 365 geht in die nächste Runde, Ende November haben die Datenschutzbehörden erneut grundlegende Bedenken geäußert. Wir haben in unserem ersten Beitrag aufbereitet, was dies für Ihr Unternehmen bedeutet (mit aktuellen Informationen zum US-Transfer personenbezogener Daten).

Unsere weiteren Beiträge beschäftigen sich mit dem Auskunftsrecht aus Art. 15 DSGVO – diesmal in Klausuren aus dem Staatsexamen, dem möglichen Verschwinden der Cookie-Banner und der Vorratsdatenspeicherung – welche Daten dürfen und müssen Telekommunikationsunternehmen von ihren Kunden künftig noch erheben und an Sicherheitsbehörden herausgeben? Schließlich haben wir im „Zu guter Letzt" wieder bemerkenswerte Bußgeldfälle zusammengetragen, auch in Sachen Meta (Facebook).

Wir wünschen Ihnen nun einen erfolgreichen Endspurt und dann besinnliche Weihnachtstage und einen energiegeladenen Start ins neue Jahr. Herzlichen Dank für Ihr Interesse an unseren Beiträgen in diesem Jahr – wir freuen uns auf den weiteren Austausch in 2023!

Wenn Ihnen unsere Inhalte gefallen, empfehlen Sie uns gerne weiter. Aktuelle Informationen gibt es auch regelmäßig in unserem Blog **www.digitalisierungsrecht.eu** – schauen Sie dort gerne einmal vorbei.

Wir freuen uns über Ihr Interesse!

Inhalt

Ist MS365 jetzt verboten? Zum Schlagabtausch zwischen Microsoft und DSK

Eine weitere unendliche Geschichte bahnt sich im Datenschutzkosmos an: Die Konferenz der unabhängigen Datenschutzbehörden (DSK) hat am 25. November 2022 erneut in einer vielbeachteten Stellungnahme die Datenschutzkonformität von Microsoft 365 infrage gestellt. Microsoft hat darauf prompt geantwortet und der DSK eine praxisferne Auslegung der DSGVO vorgeworfen. Microsoft gehe „über die rechtlichen Anforderungen hinaus, um die Daten seiner Kunden zu schützen". Die Datenschutzbehörden sehen das anders. Aber was steckt hinter der neuen Runde im Schlagabtausch zwischen Microsoft und DSK und was bedeutet dies für Unternehmen, die MS365 einsetzen?

Was bisher geschah: Die DSK hat bereits im September 2020 eine datenschutzrechtliche Bewertung von Office 365 (mittlerweile umbenannt in Microsoft 365, kurz auch „MS365") vorgenommen. Sie kam damals zu dem Ergebnis, dass ein datenschutzkonformer Einsatz von Office 365 nicht möglich sei. Die Einschätzung war ohne vorherige Anhörung von Microsoft ergangen und schon daher erheblicher Kritik ausgesetzt. Im Nachgang an diese Stellungnahme ist eine Arbeitsgruppe der DSK in einen mehrmonatigen Austausch mit Ansprechpartnern von Microsoft getreten, um die Mängel und Zweifel auszuräumen.

Im September hat Microsoft einen neuen „Datenschutznachtrag zu den Produkten und Services von Microsoft" veröffentlicht, der die Ergebnisse aus dem Austausch aufgreift. Dieses Data Protection Addendum (DPA) soll die rechtlichen Anforderungen aus Art. 28 DSGVO erfüllen. Es greift eine Reihe von Punkten aus dem Austausch zwischen Microsoft und der DSK auf.

Microsoft und DSK konnten nicht in allen Punkten Einigkeit erzielen. Die nunmehr veröffentlichten Positionen von Microsoft und DSK zur rechtlichen Einordnung des neuen DPA und der Bewertung, ob dieses für einen datenschutzkonformen Auftragsverarbeitungsvertrag ausreicht, liegen immer noch weit auseinander. Die DSK kommt unter anderem zu den Ergebnissen, dass

- nicht hinreichend eindeutig sei, welche Verarbeitungen von Microsoft durchgeführt werden und welche Daten Microsoft in eigener Verantwortung verarbeite;

- zudem die Löschvorgaben der DSGVO nicht in jedem Fall eingehalten werden könnten;

- Drittstaatenübermittlungen nicht hinreichend abgesichert seien.

Dies ist ein vernichtendes und nicht ohne weiteres zu änderndes Ergebnis und würde bedeuten, dass kein Unternehmen MS365 datenschutzrechtskonform einsetzen könnte. Allerdings: Dies ist die Position der Datenschutzbehörden. Eine gerichtliche Überprüfung derselben steht noch aus und war bisher nach unserem Kenntnisstand auch nicht möglich, da die Behörden noch keine überprüfbare Entscheidung veröffentlicht haben, sondern stets nur Positionen und Prüfergebnisse. Ob diese (verwaltungs-) gerichtlich überprüft werden können, ist umstritten.

Microsoft hält selbstbewusst dagegen. Das Unternehmen hat eine umfangreiche Stellungnahme veröffentlicht, in der es auf die Bedenken der DSK eingeht und zusätzlich eine Pressemitteilung mit dem bezeichnenden Titel *„Microsoft erfüllt und übertrifft europäische Datenschutzgesetze“*. Grundaussage ist, dass Microsoft erhebliche Anstrengungen zum Schutz der Daten seiner Kunden unternehme, man aber den Datenschutz nicht zu einem *„dogmatischen Selbstzweck“* in einer *„isolierten oder akademischen Datenschutzwelt“* werden lassen dürfe.

Auch weitere Stimmen werden laut und kritisieren die einseitige Herangehensweise der DSK (siehe etwa den FAZ-Artikel vom 11.12.2022 hier). Zudem könnte eine Klärung etwa durch ein Musterverfahren, z.B. gegen die Microsoft Deutschland GmbH, geführt werden und so auch eine gerichtliche Klärung ermöglicht werden.

Ob die DSK oder Microsoft im Recht sind, lässt sich denn auch nicht mit letzter Sicherheit sagen. In vielen Details sind die zugrundeliegenden Fragen noch nicht endgültig (höchstrichterlich) entschieden.

Davon hängen die Schlussfolgerungen für all die Unternehmen ab, die MS365 operativ einsetzen: Trifft die Ansicht der DSK zu, so

würde die Verarbeitung personenbezogener Daten aus dem Unternehmen von den Mitarbeitern, Ansprechpartnern bei Kunden und Geschäftspartnern u.U. gegen die DSGVO verstoßen. Damit verbleibt ein Bewertungsrisiko, das aus eigener Kraft kaum auszuschließen ist. In der Praxis empfehlen sich daher sauber dokumentierte Maßnahmen zur Risikoreduzierung. Wesentliche Elemente sind

- eine detaillierte, risikomindernde Konfiguration, die z.B. die LinkedIn-Integration von Mitarbeiterkonten und die Verarbeitung von Performance-Daten (Experience, Diagnose, …) durch Microsoft ausschließt;

- bei Vorhandensein eines Betriebsrates eine adäquate Betriebsvereinbarung und

- eine umfassende Risikobewertung, ggf. resultierend in eine Datenschutz-Folgenabschätzung.

Microsoft selbst gibt hierzu Hilfestellungen, etwa hier mit aktuellen Hinweisen von Ende November 2022.

Dass Microsoft und die DSK allerdings trotz intensiven Austauschs keine Einigkeit über die Anforderungen des Datenschutzes erzielen konnten, geht am Ende zu Lasten der Unternehmen/Verantwortlichen in Deutschland. Eine wirkliche Alternative zu MS365 gibt es kaum. Sie sind auf den Einsatz von Microsoft 365 angewiesen, bewegen sich dabei aber auf einem schmalen Grat. Auf absehbare Zeit wird sich daran angesichts der divergierenden Positionen von Microsoft und der DSK wohl nichts ändern.

Zumindest die Drittstaaten-Thematik aber sollte in 2023 zumindest vorerst gelöst werden. Die EU-Kommission hat am 13.12.2022 den Entwurf für einen Angemessenheitsbeschluss veröffentlicht. Sobald dieser abgestimmt und in Kraft gesetzt ist, können sich Unternehmen für einen sicheren US-Transfer darauf berufen. Etwas anderes gilt erst und nur dann, wenn der EuGH auch diesen Beschluss künftig einmal für ungültig erklären sollte – trotz aller schon verlauteten Kritik bringt diese Entscheidung damit erst einmal Sicherheit für alle Unternehmen. Daneben sollte die von Microsoft bereits angekündigte, in der Einführung aber mehrfach verschobene reine

EU-Cloud im Blick behalten werden. Auch hierzu gibt es neue Entwicklungen, allerdings noch nichts wirklich Konkretes.

BVerwG zur Einsicht in Prüfungsarbeiten

Der Auskunftsanspruch aus Art. 15 DSGVO verleiht Prüflingen im Staatsexamen nach einer aktuellen Entscheidung des BVerwG unabhängig von der Möglichkeit zur Klausureinsicht einen Anspruch auf Überlassung einer unentgeltlichen Kopie der angefertigten Aufsichtsarbeiten nebst Prüfergutachten.

Die Reichweite des datenschutzrechtlichen Auskunftsanspruches aus Art. 15 DSGVO ist immer wieder Gegenstand kontrovers geführter Diskussionen in Rechtsprechung und Literatur (siehe dazu auch unsere Blog-Beiträge hier und hier).

Das Bundesverwaltungsgericht (BVerwG) hat nun eine Entscheidung getroffen, die viele Prüfungsabsolventen freuen dürfte: Art. 15 DSGVO verleiht Prüflingen einen Anspruch auf Überlassung einer unentgeltlichen Kopie der angefertigten Prüfungsarbeiten samt Prüfergutachten.

Hintergrund

Ein Absolvent des 2. Staatsexamens aus Nordrhein-Westfalen hatte bereits 2018 von dem zuständigen Landesjustizprüfungsamt (LJPA) in Düsseldorf die Zurverfügungstellung der angefertigten Klausuren

mitsamt Prüfergutachten verlangt. Die Klausuren und deren Bewertungen seien ihm über die vom LJPA zugewiesene Kennziffer zuzuordnen und stellten damit personenbezogene Daten dar. Diese personenbezogenen Daten würden vom LJPA verarbeitet und seien daher vom Auskunftsanspruch aus Art. 15 DSGVO umfasst. Konsequenterweise hieße das, dass die Klausuren samt Prüfergutachten zur Verfügung zu stellen seien – und zwar als unentgeltliche Kopie (Art. 15 Abs. 3 S. 1 i.V.m. Art. 12 Abs. 5 S. 1 DSGVO).

Das LJPA NRW teilte diese Ansicht nicht und wollte die angeforderten Kopien nur gegen eine Gebühr von 69,70 Euro herausgeben. Begründet wurde die Ablehnung des datenschutzrechtlichen Auskunftsanspruches insbesondere damit, dass der sachliche Anwendungsbereich der DSGVO nicht eröffnet sei, da die in den Klausurbearbeitungen enthaltenen personenbezogenen Daten weder ganz noch teilweise automatisiert verarbeitet würden und auch keine Daten darstellen würden, die in einem Dateisystem gespeichert werden (nur dann ist nach Art. 2 Abs. 1 DSGVO der sachliche Anwendungsbereich der DSGVO eröffnet).

Sowohl das VG Gelsenkirchen als auch das OVG Münster sahen indes in 1. und 2. Instanz bereits die Voraussetzungen des Auskunftsanspruchs gegeben und sprachen dem Prüfling die Anspruch auf eine unentgeltliche Kopie der Klausuren mitsamt Prüfergutachten zu. Das hat das BVerwG jetzt im Ergebnis bestätigt.

DSGVO auf Prüfungsleistungen anwendbar?

Im Prozessverlauf hatte das LJPA weiter argumentiert, dass sich der datenschutzrechtliche Auskunftsanspruch nicht auf die Zurverfügungstellung sämtlicher Klausuren samt Prüfergutachten erstrecke, sondern allenfalls auf die komprimierte und verständliche Mitteilung über den Namen und die Kennziffer des Prüflings sowie auf weitere Einzelangaben wie etwa das Datum und den Ort der Prüfung oder die Note, mit der die einzelnen Aufsichtsarbeiten jeweils bewertet worden seien. Die angeforderten Dokumente beträfen zudem insgesamt 348 Seiten, weshalb der Auskunftsanspruch exzessiv und damit ausgeschlossen sei (Art. 12 Abs. 5 S. 2 DSGVO). Würde jeder Prüfling eine kostenlose Kopie seiner Klausuren verlangen dürfen, seien die personellen und sachlichen Ressourcen des LJPA überbeansprucht und eine

ordnungsgemäße Abwicklung des Prüfungsverfahrens gefährdet. Letztlich bestehe auch nach dem Juristenausbildungsgesetz NRW ein Recht zur Einsichtnahme in die Klausuren. Insofern existiere also eine Spezialvorschrift, die nach dem landesrechtlichen Datenschutzgesetz (§ 5 Abs. 8 S. 1 DSG NRW) den Anwendungsbereich von Art. 15 DSGVO ausschließe.

Das BVerwG teilte nun jedoch die Ansicht der Vorinstanzen und gab dem Prüfling Recht: Die schriftlichen Prüfungsleistungen in einer berufsbezogenen Prüfung und die dazugehörigen Anmerkungen der Prüfer stellen personenbezogene Daten dar und sind vom Auskunftsanspruch aus Art. 15 DSGVO erfasst. Der Anspruch erstreckt sich auf die Überlassung einer unentgeltlichen Kopie dieser Prüfungsunterlagen (Art. 12 Abs. 5 S. 1 i.V.m. Art. 15 Abs. 3 S. 2 DSGVO).

Prüfungsleistungen als personenbezogene Daten

Das BVerwG bezieht sich in seiner Entscheidung auf ein EuGH Urteil aus dem Jahr 2017, das noch zu der Datenschutzrichtlinie ergangen ist, die der DSGVO vorausging. Dort hatte der EuGH zu dem im Wesentlichen inhaltsgleichen Begriff der personenbezogenen Daten entschieden, dass hierunter potentiell alle Arten von Informationen fallen, z. B. in Form von Stellungnahmen oder Beurteilungen, wenn es sich um Informationen „über" die in Rede stehende Person handelt.

Die im Rahmen des zweiten juristischen Staatsexamens angefertigten Prüfungsarbeiten erfüllten diese Voraussetzungen, da sie – Wort für Wort – Informationen über die Leistungen des Prüflings enthielten. Da die Prüfung unter Zuweisung einer Kennziffer durchgeführt wird, handelt es sich bei den Prüfungsleistungen um pseudonymisierte Daten, die durch das LJPA zweifelsfrei einem Prüfling zuzuordnen werden könne. Insofern liegt auch eine teilweise automatisierte Datenverarbeitung seitens des LJPA vor, denn die Klausuren werden zwar in Papierform in der Akte des jeweiligen Prüflings aufbewahrt – ihr Auffinden und die Zuordnung zu der dahinterstehenden natürlichen Person erfolgt aber über die elektronische Datenverarbeitung mittels der jeweiligen Kennziffer.

Keine Ausschlussgründe

Die Geltendmachung des datenschutzrechtlichen Auskunftsanspruches war auch nicht als exzessiv zu bewerten: Der beim LJPA verursachte Aufwand, insgesamt 348 Seiten zu kopieren und herauszugeben, ist nach Ansicht des BVerwG als vergleichsweise gering zu qualifizieren. Auch ändert ein spezialgesetzliches Akteneinsichtsrecht nichts am Bestehen des Auskunftsanspruchs aus Art. 15 DSGVO. Der datenschutzrechtliche Auskunftsanspruch besteht unabhängig von anderen Ansprüchen und Möglichkeiten, Prüfungsarbeiten und Bewertungen einzusehen.

Verschwinden jetzt die Cookie-Banner?

Auf nahezu jeder Website, die ein Nutzer erstmals besucht, erscheint es: Ein Cookie-Banner, das den Zugriff auf die eigentlich gewollten Inhalte der Website zunächst einmal sperrt. Das Cookie-Banner ist zumeist lästig, wenn es auch einen wichtigen Zweck erfüllt: Es schützt unsere Selbstbestimmtheit über die Verarbeitungsprozesse im Internet. Aber muss dafür auf jeder Website eine Flut an Informationen auf uns einprasseln? Womöglich ändert sich das bald: Nach dem Entwurf für eine Einwilligungsverwaltungsverordnung (EinwVO-E) kommen bald „PIMS", die das Cookie-Banner auf jeder Website ersetzen. Für Publisher und Online-Vermarkter heißt es jetzt aufgepasst: Der Entwurf ist höchst kritisch zu bewerten (übrigens auch aus Nutzersicht).

Anbieter von Webseiten, Apps und anderen Telemedien benötigen die Einwilligung ihrer Nutzer, wenn sie auf deren Endgeräte zugreifen wollen, Informationen auslesen und Daten etwa für personalisierte Werbung verarbeiten. Nur, wenn das jeweilige Tool unbedingt erforderlich zum Ausspielen des Dienstes ist, kann auf die Einwilligung verzichtet werden. Diese auf eine EU-Richtlinie zurückgehende Regelung in § 25 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) ist Grund für die Cookie-Banner, die auf jeder Webseite erscheinen.

Gibt es da nicht eine bessere Lösung als unzählige Cookie-Banner, die den Zugriff auf die Seiten und Dienste erstmal verhindern? Nutzerfreundlich ist das kaum, obwohl es doch gerade die Selbstbestimmtheit der Nutzer schützen soll.

Das hat auch der Gesetzgeber gesehen und bei Verabschiedung des TTDSG im Juni 2021 die Grundlage gelegt: Personal Information Management Systeme, kurz „PIMS", sollten die Lösung werden. Der Gesetzgeber hat die Basis dafür in § 26 TTDSG gelegt und die nähere Ausgestaltung einer Rechtsverordnung überantwortet. Diese Rechtsverordnung liegt inzwischen im Entwurf vor. Und ist enttäuschend. Aber fangen wir vorne an:

Personal Information Management Systems (PIMS) als anerkannte Dienste

Die geplante Verordnung soll einen Regelungsrahmen schaffen, mit dem sich PIMS-Anbieter als anerkannte Dienste akkreditieren lassen können. PIMS werden dann im Browser des Nutzers verankert und sollen eine zentrale, generelle Einstellung ermöglichen, ob etwa ein Nutzer personenbezogene Werbung wünscht oder bestimmten Analysetools zustimmt. Webseiten, Apps etc. sollen verpflichtet werden, diese Einstellungen zu berücksichtigen, solange sie von einem akkreditierten PIMS ausgegeben werden. Nutzer könnten so sicherstellen, dass die einzelnen Angebote keine gesonderten Cookie-Banner mehr ausspielen, für ein störungsfreies Surf-Erlebnis.

Ziel der PIMS ist es also, dass Nutzer lediglich einmalig entscheiden und dann surfen, ohne auf jeder Website ein Cookie-Banner anklicken zu müssen. Aber funktionieren derart generelle Einwilligungen? Dies wird eine Herausforderung für PIMS-Anbieter, die zumindest eine Kategorisierung von Webseiten vorsehen sollten. Denn auf einer Blog-Seite mit privatem

Engagement und der Zeitungsseite mit redaktionellen Inhalten wird ein Nutzer womöglich der personalisierten Werbung zustimmen wollen, um deren Refinanzierung zu unterstützen, während er das bei E-Commerce-Anbietern womöglich nicht möchte. In der EinwVO-E ist daher auch angelegt, dass Einzeleinwilligungen für bestimmte Webseiten bzw. Apps etc., bestimmte Tools oder eben alternativ Gruppen möglich sein sollen (vgl. insb. § 3 EinwVO-E). Dies in verständlicher, nutzerfreundlicher und für den Durchschnittsnutzer handhabbarer Form umzusetzen wird eine Herausforderung.

Hohe Umsetzungshürden für PIMS- und Telemediendienste

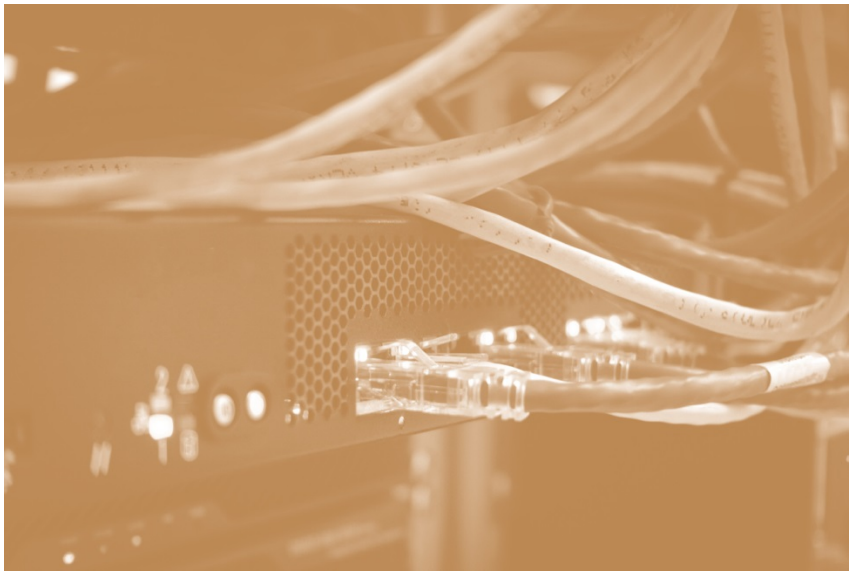
Ob sich dem eine ausreichende Anzahl von Anbietern im Markt stellen werden, bleibt abzuwarten: PIMS-Anbieter werden nur dann akkreditiert, wenn sie unabhängig von den Interessen von Webseitenanbietern etc. agieren, PIMS-Angebote von Google & Co. würden also nicht akkreditiert. Wie aber sollen sich PIMS-Anbieter dann refinanzieren? Gibt es eine Zahlungsbereitschaft der Nutzer für ein solches Angebot?

Der Akkreditierungsvorgang von PIMS-Diensten ist in §§ 6-8 EinwVO-E geregelt. Dabei wird ein umfassendes und bürokratisch aufwändiges Sicherheitskonzept gefordert. Wie genau die Bereitstellung der Information durch die Telemediendienste organisiert werden soll, ist noch offen. Dies wird technische Herausforderungen mit sich bringen, zumal die Angebote „systemoffen“ sein müssen, also mit allen auf dem Markt tätigen Diensten und Browsern kompatibel (§10 Abs. 3 EinwVO-E).

Einwilligungsnachweis

Jenseits der praktischen Umsetzbarkeit auf Seiten von PIMS-Anbietern wie auf Seite der Website- und App-Anbieter ist eine weitere Regelung in der EinwVO-E zu begrüßen, die auch jenseits von PIMS-Angeboten Auswirkungen haben könnten: § 11 EinwVO-E regelt, dass Website- und App-Anbieter das Vorliegen einer wirksamen Einwilligung nachweisen könnten, indem sie darlegen, dass ihnen die erforderliche Einwilligung über einen PIMS-Anbieter zugestellt wurde und sie zuvor dem PIMS-Anbieter die für eine wirksame Einwilligung notwendigen Informationen zur Verfügung gestellt hatten. In der Begründung heißt es sodann, dass der Nachweis während des Zugriffs vorliegen muss und durch einen

Prozessnachweis geführt werden kann (Dokumentation des Einwilligungs-Workflows). Eben dies stützt die etablierte Praxis: Nachgewiesen wird auch heute regelmäßig nicht die Einwilligung eines konkreten Nutzers, sondern schon aus Gründen der Datenminimierung nur, dass prozessual ohne Einwilligung eine Nutzung bzw. die konkrete Verarbeitung nicht möglich sein wird.



EuGH zur Vorratsdatenspeicherung

Daten über Telefonate, den Standort des Handys oder besuchte Webseiten: Anlasslos darf das nicht gespeichert werden, auch nicht für den Zugriff von Sicherheitsbehörden im Gefahrenfall. Das hat der EuGH kürzlich (erneut) entschieden und die Regelungen zur Vorratsdatenspeicherung im Telekommunikationsgesetz (TKG) für EU-rechtswidrig erklärt. Nun muss der deutsche Gesetzgeber nachbessern. Leitplanken, innerhalb derer die politische Entscheidung gefunden werden muss, ergeben sich aus dem EuGH-Urteil. Wir stellen Ihnen die Entscheidung, ihre Hintergründe und ihre Auswirkungen dar und wagen einen Ausblick auf den deutschen Gesetzentwurf, der inzwischen aus dem Bundesjustizministerium vorliegt.

Schon seit über 5 Jahren sind öffentlich zugängliche Telefondienste und Internetzugangsdienste qua Gesetz dazu verpflichtet, Verkehrs- und Standortdaten ihrer Kunden auf Vorrat allgemein und unterschiedslos zu speichern (§ 176 TKG, § 113b TKG a.F.). Zur Anwendung kamen diese gesetzliche Regelungen jedoch nie, denn die Unternehmen SpaceNet und Telekom Deutschland fochten die Speicherpflicht mit Erfolg vor den deutschen Gerichten an (u.a. OVG

Münster, Beschluss vom 22.06.2017, 13 B 238/17). Daraufhin sah die BNetzA insgesamt (gegenüber allen Verpflichteten) – bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens – von der Durchsetzung der Speicherpflicht ab (siehe Mitteilung der BNetzA).

Nach dem Urteil des EuGH am 20.09.2022 (Urteil vom 20.09.2022, C-793/19, C-794/19 – SpaceNet und Telekom Deutschland) ist nun klar: Die derzeitige Regelung zur Vorratsdatenspeicherung wird auch künftig nicht angewendet werden, da sie gegen Unionsrecht verstößt. Diese Wertung des EuGH muss das BVerwG in seinem jetzt anstehenden Urteil beachten (der EuGH hat in einem Vorabentscheidungsverfahren geurteilt).

Der EuGH bestätigt mit diesem Urteil seine bisherige Rechtsprechung zum Thema Vorratsdatenspeicherung. Insbesondere in seiner Entscheidung betreffend der britischen und der schwedischen Regelungen zur Vorratsdatenspeicherung klärte der EuGH 2016 grundlegende Rechtsfragen zur Vereinbarkeit der Vorratsdatenspeicherung mit dem Unionsrecht (EuGH, Urteil vom 21.12.2016, C-203/15 und C-698/15 - Tele2 Sverige und Watson u.a.).

Wegen weiterhin bestehender Unklarheiten und inhaltlicher Abweichungen im Vergleich zu den vorgenannten Regelungen sah das BVerwG weiterhin Klärungsbedarf in Bezug auf die deutsche Regelung und entschied sich zur Vorlage (BVerwG, Beschluss vom 25.09.2019, 6 C 12.18 und 6 C 13.18; dazu Pressemitteilung): Die deutsche Regelung erfasse weniger Kommunikationsmittel und nur bestimmte Datenkategorien (ausgenommen sind neben den Inhalten der Kommunikation, u.a. Daten über aufgerufene Internetseiten, Daten von E-Mail-Diensten, siehe § 176 Abs. 5 TKG bzw. § 113b Abs. 5 TKG a.F.). Zudem weise sie eine zeitlich enger begrenzte Speicherfrist (vier bzw. zehn Wochen) auf und enthalte strengere Beschränkungen, die den Schutz der gespeicherten Daten vor Missbrauch und unberechtigtem Zugriff gewährleisten. Außerdem sei nicht eindeutig, ob die Ausführungen des EuGH im Urteil vom 21.12.2016 als generelles Verbot einer anlasslosen Vorratsdatenspeicherung zu verstehen seien. Das BVerwG wies daraufhin, dass ein ausnahmsloses Verbot der anlasslosen Speicherung von Verkehrs- und Standortdaten auf Vorrat die Mitgliedstaaten erheblich beschränken würde, Strafverfolgung und öffentliche Sicherheit eigenständig zu regeln.

Absage an deutsche Regelung

Der EuGH sah die Besonderheiten der deutschen Regelungen, kippte diese im Ergebnis aber dennoch: Eine nationale Regelung wie die im TKG, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen für die *öffentliche* Sicherheit eine allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten vorsieht (Rn. 131), ist nicht vereinbar mit dem EU-Recht. Der von der Speicherpflicht erfasste Datensatz sei umfangreich (Rn. 81) und ermögliche auch bei einer Speicherdauer von zehn bzw. vier Wochen „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden […], und insbesondere die Erstellung eines Profils dieser Personen" (Rn. 90). Zudem seien die im TKG vorgesehenen Garantien zum Schutz gegen Missbrauch und unberechtigten Zugriff nur geeignet den Eingriff durch Zugang zu den gespeicherten Daten zu beschränken oder zu beseitigen, nicht jedoch den („naturgemäß schwereren") Eingriff der Vorratsdatenspeicherung (Rn. 91)

Welche Regelungen wären unionsrechtskonform?

Ein allgemeines Verbot der anlasslosen Vorratsdatenspeicherung sprach der EuGH dagegen nicht aus. Eine **allgemeine und unterschiedslose** Speicherung von Verkehrs- und Standortdaten auf Vorrat kann nach der EuGH-Entscheidung in folgenden Ausnahmefällen und unter Beachtung der genannten Voraussetzungen sowie des Grundsatzes der Verhältnismäßigkeit mit dem Unionsrecht vereinbar sein:

- **Nur zeitlich begrenzt bei ernster Bedrohungslage:** Allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten auf Vorrat nur auf Anordnung zum Schutz der *nationalen Sicherheit*, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden *ernsten Bedrohung* für die nationale Sicherheit gegenübersieht, der Zeitraum, auf den sich die Anordnung erstreckt, auf das absolut Notwendige begrenzt ist und die Anordnung durch ein Gericht oder eine unabhängige Verwaltungsstelle (mit Bindungswirkung) kontrolliert werden kann (Rn. 131, 1. Spiegelstrich).

- Allgemeine und unterschiedslose Speicherung von **IP-Adressen** auf Vorrat zum Schutz der nationalen Sicherheit, zur

Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolute Notwendige begrenzten Zeitraum (Rn. 131, 3. Spiegelstrich).

- Allgemeine und unterschiedslose Speicherung von Daten, die die **Identität der Nutzer elektronischer Kommunikationsmittel** betreffen, auf Vorrat zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit (Rn. 131, 4. Spiegelstrich).

Daneben ist eine **gezielte Vorratsdatenspeicherung** von Verkehrs- und Standortdaten zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit unionsrechtskonform, sofern die *Speicherung auf Grundlage objektiver und nichtdiskriminierender Kriterien etwa geografisch oder bezogen auf bestimmte Personenkreise eingegrenzt wurde* und sich die Speicherdauer auf ein absolut notweniges Maß begrenzt (Rn. 131, 2. Spiegelstrich).

Schließlich sind nationale Rechtsvorschriften unionsrechtskonform, die es den zuständigen Behörden gestatten, zur Bekämpfung schwerer Kriminalität und, a fortiori, zum Schutz der nationalen Sicherheit Betreibern elektronischer Kommunikationsdienste mittels **Entscheidung** aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten **umgehend zu sichern** (Rn. 131, 5. Spiegelstrich), also einen sog. Quick-Freeze durchzuführen („on the fly“).

Zudem schreibt der EuGH (in Fortführung seiner bisherigen Rechtsprechung) vor: **Klare und präzise Regeln** müssen sicherstellen, dass die geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (Rn. 131).

Was kommt nun?

Die Leitplanken hat der EuGH damit vorgegeben. Nachbessern muss der deutsche Gesetzgeber in jedem Fall. Er kann die Möglichkeiten, die das EuGH-Urteil offenlässt, voll ausschöpfen oder eine weniger eingriffsintensive Regelung wählen.

Das BMJ hat sich nun für die wohl am wenigsten eingriffsintensive Option entschieden, das sog. Quick-Freeze-Verfahren. Dazu hat das BMJ nun auch einen Gesetzesentwurf vorgelegt. Dieses Verfahren sieht vor, dass die bei den Anbietern von Telekommunikationsdiensten ohnehin bereits vorhandenen und künftig anfallenden Verkehrsdaten gesichert werden („Einfrieren"), wenn dies zur Verfolgung von erheblichen Straftaten beitragen kann. Informationen, die in den Telekommunikationssystemen vorliegen, müssen dann technisch so erhoben und abgelegt werden, dass ein späterer Zugriff möglich ist. Diese „Einfrieren" erfolgt „on the fly", d.h. bei einem entsprechenden Anlass fordert eine befugte Behörde den Telekommunikationsanbieter auf, zu sichern, welcher Person zum konkreten Zeitpunkt eine IP-Adresse zugeordnet ist, welche Verkehrs- oder Standortdaten u.ä.

Im ersten Schritt wird dabei nur die Sicherung der Daten angeordnet, ohne direkten Zugriff (§ 100g Abs. 1 StPO). Im zweiten Schritt können Behörden dann die Herausgabe fordern und damit auch auf die Daten zugreifen (§ 100g Abs. 1, 3 StPO). So soll verhindert werden, dass ermittlungsrelevante Daten gelöscht werden (mussten), bevor ausreichend Beweise vorlagen, um als Ermittlungsbehörde tatsächlich Zugriff auf diese Daten erhalten zu können. Abgesichert wird so aber, dass keine anlasslose Vorratsdatenspeicherung, unterschiedslos, erfolgt, sondern nur im Fall hinreichend konkreter Anhaltspunkte.

Die technischen Vorkehrungen für die Durchführung von Quick-Freeze-Verfahren haben Telekommunikationsanbieter auf eigene Kosten vorzusehen, wie auch bisher schon. Erreichen sie konkrete Anfragen, werden diese Kosten erstattet.

Zu guter Letzt

Zum Jahresende haben wir nochmal einige spannende Bußgeldentscheidungen und Neuigkeiten für Sie. Meta erwartet ggf. ein hohes Bußgeld, weil es die Einwilligung in die Nutzung personenbezogener Daten für benutzerspezifizierte Werbung in den AGB versteckte. Ein Bußgeld in Millionenhöhe gab es in Lettland wegen der Übermittlung ungeprüfter Informationen. Für unzulässige Cookies wurden in Spanien 525.000 Euro fällig. Diese und weitere Entscheidungen haben wir für Sie zusammengefasst und weisen zudem auf ein neues Kurzgutachten der DSK zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages hin.

- **Datenschutzverstoß durch personalisierte Werbung auf Facebook, Instagram und WhatsApp**

Der Europäische Datenschutzausschuss (EDSA) hat am 06. Dezember 2022 eine Entscheidung zu Datenverarbeitungen bei der Nutzung von Facebook, Instagram und WhatsApp getroffen. Meta hat sich in den Nutzungsbedingungen der Anwendungen jeweils das Recht vorbehalten, Daten der Nutzer zu Werbezwecken oder zur Verbesserung der Dienste zu verarbeiten, statt hierfür eine Einwilligung einzuholen. Die Irische Data Protection Commission (DPC) hat diese Praxis auf eine Beschwerde der Datenschutzorganisation NOYB aus dem Jahr 2018 hin dem EDSA vorgelegt, der nunmehr verbindlich darüber entschieden hat. Die DPC hat einen Monat Zeit, aufgrund dieser Entscheidung eine

Entscheidung gegenüber Meta zu treffen. Wie diese im Detail aussieht, ist noch unklar. In Online-Artikeln wird eine hohe Geldbuße gegenüber Meta und eine Untersagung der Praxis, Datenverarbeitungsbefugnisse durch AGB zu schaffen, erwartet (s. auch hier). Meta kann sich hiergegen dann gerichtlich wehren. Wir halten Sie zu alledem natürlich auf dem Laufenden.

- **Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages**

Die DSK hat eine neue Version des Kurzgutachtens zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages veröffentlicht. Das Kurzgutachten vom 10. November 2022 beschäftigt sich mit der rechtlichen Bewertung des Betriebs von Fanpages unter Berücksichtigung des seit dem 1. Dezember 2022 geltenden Telekommunikations-Telemedien-Datenschutzgesetztes (TTDSG), des Urteils des OVG Schleswig vom 25.11.2021 und dem aktuellen tatsächlichen Umsetzungsstand durch Facebook. Der neue Überarbeitungsstand ist etwas länger und gründlicher als die erste Version vom März 2022 und enthält Ausführungen dazu, ob eine Deaktivierung der Besucherstatistiken dazu führt, dass keine gemeinsame Verantwortung zwischen dem Betreiber und Facebook besteht.

- **Lettland: 1.200.000 Millionen Euro für Internetdiensteanbieter Tet wegen Weitergabe ungeprüfter personenbezogenen Daten**

Die lettische Datenschutzbehörde hatte zunächst eine Untersuchung über die Datenverarbeitungspraktiken des Unternehmens Tet, insbesondere die Übermittlung von Kundendaten an außergerichtliche Inkassodienstleister, eingeleitet. Hierbei stellte sich heraus, dass der Internetdiensteanbieter Bonitätsprüfungen zur Vorbereitung eines Vertragsschlusses bei einem Inkassodienstleister durchführen ließ, jedoch ohne vorherige Identitätsprüfung der betroffenen Personen. Aus diesem Grund wurden in einem Fall personenbezogene Daten eines Minderjährigen an den Inkassodienst übermittelt, weil die Richtigkeit der von einem Kunden gemachten Angaben zuvor nicht überprüft wurden. Hierin sah die Datenschutzbehörde einen Verstoß gegen die Datenverarbeitungsgrundsätze der Rechtmäßig und Richtigkeit (Art. 5 Abs. 1 lit. a) und d) DSGVO).

Darüber hinaus gab der für die Verarbeitung Verantwortliche die personenbezogenen Daten der betroffenen Person (Vorname, Nachname, Geburtsdatum und Wohnanschrift) an Dritte weiter, indem er Dokumente mit ungeprüften und unrichtigen personenbezogenen Daten in das interne Kundenselbstbedienungssystem unter dem jeweiligen Benutzerkonto einstellte. Hierin sah die lettische Datenschutzbehörde einen Verstoß gegen die Grundsätze der Richtigkeit und der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. a) und f) DSGVO).

Die DPA verhängte gegen den für die Verarbeitung Verantwortlichen ein Bußgeld i.H.v. 3.200.000 Euro. Unter Berücksichtigung mildernder Umstände, insbesondere der Kooperationsbereitschaft des Unternehmens sowie der zur Behebung der Verstöße ergriffenen Maßnahmen, wurde dies auf 1.200.000 Euro reduziert. Tet hat mittlerweile bekannt gegeben, gegen die Entscheidung gerichtlich vorgehen zu wollen.

- **Spanien: 525.000 Euro Bußgeld für TECHPUMP SOLUTIONS S.L.**

Aufgrund von Hinweisen bezüglich Datenschutzverstößen untersuchte die spanische Datenschutzbehörde die Websites des Unternehmens TECHPUMP SOLUTIONS S.L., welche mehrere Websites mit Erwachseneninhalten betreibt. Hierbei stellte die Datenschutzbehörde unter anderem fest, dass es nicht möglich war Cookies auf der Website zu deaktivieren. Die Datenschutzerklärung und AGB waren zudem ausschließlich in englischer Sprache verfügbar, konnten nicht im Rahmen der Anmeldung eingesehen werden und enthielten zudem keine hinreichend klare Beschreibung der durchgeführten Datenverarbeitungen. Darüber hinaus forderte die Website zur Löschung von personenbezogenen Daten die Vorlage des Personalausweises der Nutzer und es lag kein ausreichender Schutz minderjähriger Nutzer vor.

Diese Datenschutzverstöße sanktionierte die spanische Datenschutzbehörde mit einem Bußgeld in Höhe von 525.000 Euro.

- **Frankreich: Der Messaging-Dienst DISCORD erhielt 800.000 Euro Bußgeld wegen mehrerer Verstöße gegen die DSGVO.**

DISCORD ist ein Instant-Messaging-Dienst, bei dem die Nutzer über ihr Mikrofon und ihre Webcam chatten und (video-)telefonieren können. Hierzu können diese Text-, Sprach- und Videoräume einrichten.

Die französische Datenschutzbehörde (CNIL) stellte bei einer Untersuchung fest, dass das Unternehmen gegen mehrere Pflichten aus der DSGVO verstoßen hat.

Es wurde wegen Nichtfestlegung und Nichteinhaltung einer dem Zweck angemessenen Aufbewahrungsfrist für Daten gegen den Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) verstoßen. Zudem verstieße das Unternehmen gegen die Informationspflichten aus Art. 13 DSGVO, da es keine vollständigen Informationen über Aufbewahrungsfristen bereitstellte. Die Anwendung wurde zudem durch klicken auf das "X"-Symbol oben rechts im Fenster von Microsoft Windows nicht beendet, sondern lief im Hintergrund weiter. Benutzer konnten somit teilweise von anderen Mitgliedern im Sprachraum gehört werden, obwohl sie davon ausgingen, die Funktion beendet zu haben. Einen Hinweis darauf gab es nicht. Die CNIL erkannte hierin einen Verstoß gegen die Verpflichtung, durch Technikgestaltung und durch angemessene technisch-organisatorische Maßnahmen ein angemessenes Datenschutzniveau zu gewährleisten.

Während des Verfahrens ergriff DISCORD bereits Maßnahmen, wodurch die festgestellten Verstöße gegen die DSGVO nunmehr unterbunden werden sollen.

Die Datenschutzbehörde verhängte ein Bußgeld von 800.000 Euro.

- **Der französische Stromversorger EDF France muss 600.000 Euro Bußgeld zahlen**

Grund hierfür ist, dass der Stromanbieter es versäumt hatte die Zustimmung bezüglich des Erhalts von Werbeprospekten per E-Mail einzuholen und somit gegen Art. 7 DSGVO verstieß. Das Unternehmen gewährleistete zudem keine ausreichende Sicherheit für personenbezogene Daten und informierte Betroffene nicht ausreichend. Außerdem ist EDF seinen Verpflichtungen aus dem

französischen Gesetz über Post und elektronische Kommunikation nicht nachgekommen. Dies stellte sich bei den Untersuchungen der französischen Datenschutzbehörde (CNIL) heraus, welche aufgrund zahlreicher Beschwerden durch Einzelpersonen auf das Unternehmen aufmerksam wurde. Die CNIL ahndete die Verstöße mit einem Bußgeld i. H. v. 600.000 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

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