LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2021

Sehr geehrte Damen und Herren,

trotz erneutem Böllerverbot haben wir gleich zu Beginn eine Gerichtsentscheidung mit enormer Sprengkraft für Sie: Das VG Wiesbaden untersagt den Einsatz der bekannten und weit verbreiteten Anwendung Cookiebot, da dieser auf Server eines US-Unternehmens zurückgreift. Die Übermittlung der IP-Adresse reiche für die Untersagung aus.

Und auch die Datenschutzkonferenz hat eine Entscheidung mit enormer Tragweite für die Praxis veröffentlicht: Eine individuelle Einwilligung in ein verringertes Datensicherheitsniveau soll rechtlich kaum zulässig sein. Darüber hinaus berichten wir über die Offenlegung von Bußgeldbescheiden, die Entwicklungen der EU-Digitalstrategie und interessante Bußgelder aus anderen Mitgliedstaaten.

Ganz herzlich möchten wir uns an dieser Stelle für Ihr Interesse an unserem Newsletter in diesem Jahr bedanken. Wir wünschen Ihnen ein frohes und besinnliches Weihnachtsfest und alles Gute für das neue Jahr 2022!

Inhalt

Cookiebot und das Content Delivery Network Akamai vor dem Aus? VG Wiesbaden zum Drittstaatentransfer nach Schrems II

Ein Knaller zum Jahresende: Das VG Wiesbaden untersagt der Hochschule RheinMain vorläufig den Einsatz des bekannten und weit verbreiteten Consent Management Tools „Cookiebot“: Die Nutzung des Dienstes, mit dem Einwilligungen in die Cookie-Verwendung abgefragt werden können, führe zu einem unzulässigen Drittstaatentransfer. Die Entscheidung des VG Wiesbaden ist zudem die erste veröffentlichte Gerichtsentscheidung zum Drittstaatentransfer personenbezogener Daten nach dem Schrems II-Urteil des EuGH.

Seit der EuGH am 16.07.2020 in Sachen *Schrems II* geurteilt hat, besteht in Europa eine große Unsicherheit darüber, ob und inwiefern die Nutzung US-amerikanischer Tools datenschutzrechtlich zulässig ist. Der EuGH hatte mit der Schrems II-Entscheidung das EU-US-Privacy Shield, einen Angemessenheitsbeschluss für den Datentransfer in die USA, für ungültig erklärt und die Verwendung von Standardvertragsklauseln einer besonderen Prüfpflicht unterworfen, die für die USA ohne zusätzliche Maßnahmen kaum zu einem positiven Ergebnis führen konnte. Im Juni 2021 hatten die deutschen Aufsichtsbehörden dann mit einer Schwerpunktprüfung „Drittenstaatentransfer“ begonnen (wir berichteten hierzu in unserem Newsletter vom Juni 2021). Nun folgte am 01.12.2021 die (soweit ersichtlich) erste Gerichtsentscheidung zu der Problematik in Deutschland (VG Wiesbaden, Beschluss vom 01.12.2021, Az. 6 L 738/21.WI).

Das Verfahren

Im Zuge eines Eilverfahrens hatte das VG Wiesbaden darüber zu entscheiden, ob die Hochschule RheinMain weiterhin den bekannten und weit verbreiteten Dienst Cookiebot einsetzen darf, um die Cookie-Einwilligungen ihrer Website-Nutzer zu verwalten. Geklagt hatte ein Nutzer, der auf der Website der Hochschule regelmäßig Literaturrecherche betreibt. Der Dienst Cookiebot wird zwar von einem dänischen Unternehmen angeboten, dieser nutzt mit dem Content Delivery Network von Akamai allerdings von einem US-Anbieter gehostete Server, um den Dienst bereitzustellen.

Der Cookiebot dient dem Speichern und Verwalten der Entscheidungen von Nutzern über die Verwendung von Cookies. Hat der Nutzer etwa der Erhebung von Marketing-Cookies nicht zugestimmt, merkt sich Cookiebot durch einen auf dem Endgerät des Nutzers abgelegten Consent-Cookie die Entscheidung und berücksichtigt diese beim nächsten Besuch des Nutzers. Mit anderen Worten: Cookiebot nutzt seinerseits Cookies, um seinen Service anbieten zu können. Das können Sie im Selbstexperiment einmal über die Cookie Suche Ihres Browsers nachvollziehen.

Um das Banner des Cookiebot anzuzeigen, ist es technisch notwendig, die vollständige IP-Adresse an den US-Server von Akamai zu übermitteln. Da die IP-Adresse die eindeutige Identifizierung des Nutzers ermögliche, handele es sich bei ihr – so das VG Wiesbaden – um ein personenbezogenes Datum.

Übermittlung der IP-Adresse

Schon die Übertragung der ungekürzten IP-Adresse beim erstmaligen Laden eines Dienstes stellt nach Ansicht des VG Wiesbaden eine datenschutzrechtlich beachtliche Verarbeitung dar. Dabei soll es nach Ansicht des Gerichts sogar unerheblich sein, ob die Server von Akamai in der EU oder den USA belegen sind: Allein entscheidend sei, dass der Server-Host als US-amerikanisches Unternehmen dem sog. Cloud-Act unterliege, der ihn dazu verpflichte, US-Behörden auf Anfrage Daten offenzulegen. Der Beschluss des Verwaltungsgerichts zeigt damit auf, wie schnell ein US-Bezug mit Datentransfer i.S.d. Art. 44 DSGVO bestehen kann.

Die Hochschule sei für all dies auch datenschutzrechtlich verantwortlich: Für die Verantwortlichkeit reiche es aus, dass sich die Hochschule für die Nutzung des Dienstes entschieden hatte und diesen bewusst einsetze.

Keine geeigneten Garantien

Auf der Website der Hochschule werde weder eine Einwilligung für eine Drittstaatenübertragung eingeholt, noch über die Risiken des US-Cloud Acts aufgeklärt. Die Übertragung der Cookie-Entscheidung des Nutzers in die USA sei auch nicht erforderlich für den Betrieb der Website. Weder Art. 48 noch Art. 49 DSGVO erlaubt den Datentransfer hier.

Ob die zwischen dem Anbieter des Cookiebot und Akamai abgeschlossenen Standardvertragsklauseln geeignete Garantien darstellen könnten, wird in der Entscheidung des VG Wiesbaden nicht erörtert.

Die Entscheidung

Aus diesen Gründen hat das Gericht der Hochschule auferlegt, den Cookiebot-Dienst von ihrer Website zu entfernen. Der Beschluss ist noch nicht rechtskräftig, da noch eine Beschwerde zum Hessischen Verwaltungsgerichtshof in Kassel möglich ist. Zudem steht die Entscheidung unter dem Vorbehalt des Hauptsacheverfahrens, welches innerhalb von 4 Wochen einzuleiten ist.

Kritik

Die Entscheidung des VG Wiesbaden hat enorme Sprengkraft für die Praxis: Setzt sich die Ansicht des Gerichts durch, könnten etliche Online-Tools nicht mehr genutzt werden. Viele Angebote fußen auf den Angeboten von US-Unternehmen, die IP-Adresse wird stets benötigt, um die Angebote dem Nutzer überhaupt technisch anzeigen zu können.

Ob in der Beschwerdeinstanz oder jedenfalls dem Hauptsacheverfahren die Entscheidung des VG Wiesbaden bestätigt wird, ist fraglich. Insbesondere versäumt es das Gericht, zu prüfen, ob die Standardvertragsklauseln hier geeignete Garantien liefern könnten. Die neuen Standardvertragsklauseln vom 04.06.2021 sehen ausdrücklich eine Risikobetrachtung vor: Maßgeblich ist nicht nur, ob nationale Rechtsvorschriften Behördenzugriffe ermöglichen, die mit dem EU-Standard nicht vereinbar sind – dies wäre für die USA nach der EuGH-Entscheidung in Sachen *Schrems II* zu bejahen. Entscheidend ist darüber hinaus, ob nach den praktischen Erfahrungen auch tatsächlich mit derartigen Zugriffen zu rechnen ist. Dies haben die US-Behörden für den Fall der IP-Adresse bereits verneint: An diesen Informationen bestehe kein Interesse.

Die Entscheidung des VG Wiesbaden dürfte damit in der Praxis nicht dazu führen, dass unverzüglich jegliche US-Bezüge im vorbenannten Sinn zu beenden sind. Sie verdeutlicht aber erneut, wie groß die bestehende Rechtsunsicherheit ist und wie wichtig die Durchführung von Transfer Impact Assessments, also der umfassenden Risikobewertung von Drittstaatentransfers, ist. Dies ist

auch dann notwendig, wenn ein eingesetzter EU-Dienstleister wie hier seinerseits als Unterauftragsverarbeiter auf US-Unternehmen zurückgreift. Typische Anwendungsfälle hierfür sind auf die Angebote von Akamai, Amazon, Microsoft oder Google aufbauende Tools.

Können Betroffene auf ein „angemessenes Datensicherheitsniveau“ verzichten?

Die Datenschutzkonferenz hat dem am 24. November 2021 mit einem neuen Beschluss eine recht klare Absage erteilt. Relevant ist dies z.B. für die Übermittlung sensibler Daten per Email, die immer wieder auf datenschutzrechtliche Bedenken stößt. Im Frühjahr 2021 hatte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sich dazu noch abweichend positioniert und die Möglichkeiten für eine Einwilligung in ein niedrigeres Datensicherheitsniveau dargelegt. Was gilt nun?

„Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.“

So eindeutig beginnt der neue Beschluss der Datenschutzkonferenz vom 24.11.2021. Damit stellt sich die DSK gegen die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HamBfDI) noch als möglich angesehene Einwilligung in ein geringeres Datensicherheitsniveau. Der HamBfDI hatte in seinem Vermerk aus dem Frühjahr 2021 dazu Stellung bezogen, ob Betroffene auf das nach Art. 32 DSGVO erforderliche Datensicherheitsniveau verzichten können.

Ein typischer Anwendungsfall in der Praxis ist die Frage, ob sensible Daten wie Gesundheitsdaten oder Steuerinformationen von Ärzten, Anwälten oder Steuerberatern per Email ohne eine Ende-zu-Ende-Verschlüsselung verschickt werden dürfen, wenn die betroffene Person damit einverstanden ist, eigentlich aber nach Art. 32 DSGVO die Verschlüsselung erfolgen müsste.

Zur Erinnerung: Art. 32 DSGVO gibt Datenverarbeitern, Verantwortlichen wie Auftragsverarbeitern, vor, ein für die Datenverarbeitungssituation angemessenes Niveau der Datensicherheit zu schaffen. Dies hat der Datenverarbeiter durch Abwägung der Risiken der Verarbeitung, der Implementierungskosten und der Art, Weise und des Umfangs der Datenverarbeitung zu ermitteln und entsprechende Maßnahmen zu treffen. Das Niveau und die zu treffenden Maßnahmen sind dabei nicht abschließend vorgeschrieben, sondern risiko- und situationsabhängig in eigener Verantwortung zu prüfen und festzulegen. Bei der Übermittlung sensibler Daten wie Gesundheitsdaten per Email wird es regelmäßig erforderlich sein, dass die Email-Kommunikation Ende-zu-Ende verschlüsselt ist. Eine reine Transportverschlüsselung ist regelmäßig nicht ausreichend. Zu datenschutzrechtlichen Problemen führt es, wenn eine der beiden Seiten dieses Verschlüsselungsniveau nicht einhalten kann oder will. In diesen Fällen stellt sich die Frage, ob solche Daten trotzdem versendet werden dürfen, wenn der Betroffene darin einwilligt.

Stellenwert der Selbstbestimmungsrechte der Betroffenen in Bezug auf Art. 32 DSGVO aus Sicht des HamBfDI

Die hier zu beantwortenden Rechtsfragen berühren die Grundfesten des Datenschutzrechts. Die DSK hält eine Einwilligung nach ihrem neuen Beschluss nur in dokumentierten Einzelfällen für denkbar, wenn der Betroffene ausdrücklich und eigeninitiativ darum bittet.

Nach der Analyse des HamBfDI ist dies eine Frage des (informationellen) Selbstbestimmungsrechts über personenbezogene Daten. Zwar sei es das Ziel der DSGVO, ein allgemeines, möglichst hohes und einheitliches Schutzniveau für personenbezogene Daten zu schaffen. Gleichzeitig solle aber auch das individuelle Selbstbestimmungsrecht der Betroffenen über ihre personenbezogenen Daten geschützt werden. Zum Selbstbestimmungsrecht gehört es nach Ansicht des HamBfDI auch, Entscheidungen darüber zu treffen, Daten unter einem suboptimalen Schutz verarbeiten zu lassen. Der HamBfDI vergleicht dies mit der Veröffentlichung sensibler Daten: Diese möge zwar in manchen Fällen nicht die objektiv klügste Entscheidung sein, es stehe dem Einzelnen aber zweifelsohne zu und es ist von der Rechtsordnung gedeckt, solche unklugen Entscheidungen über seine personenbezogenen Daten ohne Bevormundung zu treffen. So solle es sich auch mit der Entscheidung über ein niedrigeres Schutzniveau bei der Datenübertragung verhalten.

Die DSK sieht dies nun deutlich restriktiver und begrenzt diese Fälle auf solche, in denen der Betroffene die Initiative ergreift. Dies dürfte systematische Angebote, in ein niedrigeres Schutzniveau einzuwilligen, ausschließen.

Jedenfalls: Verpflichtung der Verarbeiter

Selbst wenn danach dem Betroffenen die freie Entscheidung zugebilligt wird, ein niedrigeres Schutzniveau für seine personenbezogenen Daten zu wählen, bleiben die verantwortlichen Datenverarbeiter nach Art. 32 DSGVO verpflichtet, ein geeignetes und angemessenes Niveau sicherzustellen und anzubieten. Dabei merkt der HamBfDI an, dass es für die Bestimmung des Niveaus nicht auf den Einzelfall, sondern auf das typische, für solche Verarbeitungssituationen angemessene Niveau ankommt. Deshalb müssten Datenverarbeiter stets und unabhängig von dem möglichen Willen einzelner Betroffener die Vorkehrungen treffen, die zur Einhaltung des angemessenen Niveaus erforderlich sind. Im konkreten Fall der Email-Kommunikation heißt das, dass die Ende-zu-Ende-Verschlüsselung zumindest auf der eigenen Seite technisch und operationell ermöglicht werden muss.

Dadurch wird nach Ansicht des HamBfDI dann auch die Freiwilligkeit der Betroffenen gewahrt: Diese können zwischen einem angemessenen und abgesenkten Schutzniveau frei

entscheiden, auch, weil der Verpflichtete auch ein angemessenes Schutzniveau anbietet. Die Einwilligung in ein suboptimales Schutzniveau ist nicht notwendig, um die Leistung erhalten zu können. Problematisch sind also dann vor allem solche Geschäftsmodelle, im Rahmen derer keine angemessenen Maßnahmen umgesetzt werden. Die Freiwilligkeit könnte sich dann allenfalls in der freiwilligen Teilnahme widerspiegeln. Dieses Problem potenziert sich, wenn es sich um Anwendungen handelt, die für die Betroffenen dringend notwendig sind und/oder keine Alternativen am Markt bestehen. Für die DSK reicht dies nicht – hier muss für eine wirksame Einwilligung zudem die Initiative vom Betroffenen ausgehen.

Einwilligung in niedrigeres Niveau möglich?

Nach der DSK ist eine Einwilligung in ein niedrigeres Datensicherheitsniveau damit nur in vereinzelten Ausnahmefällen zulässig. Der HamBfDI hatte dies noch weiter gesehen. In jedem Fall muss eine Einwilligung die Voraussetzungen der Art. 6 Abs. 1 UAbs 1 lit. a, Art. 7 DSGVO erfüllen, also insbesondere nach angemessener Aufklärung dokumentiert für den Einzelfall erteilt werden.

Noch einmal zusammengefasst bestehen also die folgenden Voraussetzungen:

1. Der Verantwortliche oder Auftragsverarbeiter hat das erforderliche Datensicherheitsniveau nach Maßgabe des Art. 32 DSGVO geschaffen. Die Möglichkeit der Einwilligung des Betroffenen soll nicht genutzt werden, um Kosten zu sparen und den Betroffenen niedrigere Datensicherheit „aufzudrücken".

2. Die Einwilligung des Betroffenen muss die strengen Anforderungen der Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO und Art. 7 DSGVO erfüllen, bei sensitiven Daten auch des Art. 9 Abs. 2 lit. a DSGVO. Insbesondere muss die Einwilligung freiwillig und informiert erfolgen.

3. Die Einwilligung muss, nach DSK-Position, im Einzelfall ausdrücklich auf Initiative des Betroffenen abgegeben werden. Systematische Angebote dürften damit nicht vereinbar sein.

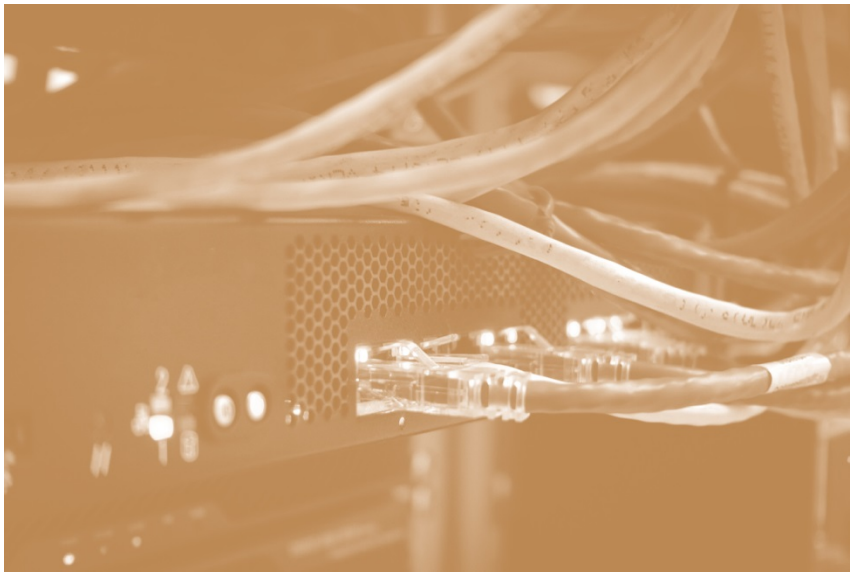
Der DSK-Beschluss begrenzt die Möglichkeiten damit erheblich

Kritik

Die Position der DSK ist mit Blick auf das informationelle Selbstbestimmungsrecht kritikwürdig: Es überzeugt kaum, dass Betroffene zwar in die Datenverarbeitung als solche einwilligen können, nicht aber in ein reduziertes Sicherheitsniveau. In der Praxis darf mithin der Arzt auch auf Anforderung des Patienten die Gesundheitsunterlagen nicht per einfacher Email übersenden. Ob sich diese Ansicht durchsetzt, ist fraglich – ein Beschluss der DSK jedenfalls bindet weder Verantwortliche, noch Aufsichtsbehörden. Er markiert indes das Risiko, ob Aufsichtsbehörden gegen eine bestimmte Verarbeitung einschreiten werden oder nicht. Gleichzeitig wird man die DSGVO auch im europäischen Kontext und ggf. losgelöst von der deutschen Grundrechtstheorie verstehen müssen. Die Diskussion ist an dieser Stelle ganz sicher nicht beendet.

Der Vermerk des HamBfDI ist abrufbar unter:
https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf

Der Beschluss des DSK ist abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf



Keine Veröffentlichung von Bußgeldbescheiden

Die Anwendung der DSGVO ist auch über 3 Jahre nach ihrem Inkrafttreten noch in etlichen Details unklar. Gerichtsentscheidungen sind rar. Weiterführende Hinweise zur konkreten Anwendung der Vorgaben könnten sich aus Bußgeldbescheiden der Datenschutzaufsichtsbehörden ergeben. Aber besteht ein Informationsanspruch Dritter, ein Anspruch auf Offenlegung eines Bußgeldbescheides? Das Landgericht Hamburg verneint dies.

Mit Urteil vom 28.10.2021, Az. 625 Qs 21/21 OWi, lehnte das LG Hamburg die Offenlegung des gegen H&M ergangenen Bußgeldbescheids des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HamBfDI) auch in anonymisierter Form ab. Mehrere Zugangsersuchen hatten den HamBfDI nach Erlass des Bußgeldbescheids erreicht. Besonderes Interesse galt den Erläuterungen zur Bußgeldbemessung. Zur Erinnerung: Gegenüber H&M war wegen Spitzelvorwürfen ein Bußgeld in Höhe von 35 Mio. Euro verhängt worden.

Gemäß § 475 Abs. 1, 4 StPO können Privatpersonen Auskünfte aus Akten erteilt werden, soweit diese hierfür ein berechtigtes Interesse darlegen. Sie sind zu versagen, wenn der hiervon Betroffene ein schutzwürdiges Interesse an der Versagung hat. Letzteres steht nach Ansicht des LG Hamburg einer Auskunftserteilung hier entgegen: Zwar bestünden berechtigte Interessen an den Informationen. H&M habe aber schutzwürdige Interessen an der Versagung, etliche Informationen seien als Betriebs- und Geschäftsgeheimnisse geschützt, auch Art. 12 GG stehe der Zugangsgewährung entgegen. Im Einzelfall kann dies auch das Unternehmenspersönlichkeitsrecht gem. Art. 2 Abs.1 GG sein.

Letztlich ist dies eine Einzelfallentscheidung, die indes richtungsweisend in der andauernden Auseinandersetzung um die Offenlegung von Bußgeldentscheidungen ist: Betroffene Unternehmen sind schutzwürdig, Informationen über verhängte Bußgelder unterliegen nicht der freien Veröffentlichung.

Die europäische Datenstrategie – EDSA übt Kritik an geplanter EU-Datengesetzgebung

Aus Brüssel kommen neue Rechtsakte zu digitalen Themen am Fließband: Vom Digital Governance Act bis zur Künstliche-Intelligenz-Verordnung ist in Sachen Datengesetzgebung viel in Bewegung. Aber sind die geplanten Regelungen auch DSGVO-konform? Werden die Grundrechte gewahrt und fügen sich in ein stimmiges Gesamtkonzept ein? Der Europäische Datenschutzausschuss (EDSA) meint: Nein. Die Kritik ist grundlegend und sollte gehört werden.

Die EU setzt ihre Digitalstrategie um: Schlag auf Schlag erscheinen neue Gesetzgebungsvorschläge. Allein im letzten Jahr veröffentlichte die Europäische Kommission die Entwürfe für vier Verordnungen, mit denen unterschiedliche Aspekte der Datenwirtschaft und datenbasierten technologischen Entwicklung adressiert werden. Dies sind:

- **Digital Governance Act** (Daten-Governance-Gesetz oder kurz DGA) aus November 2020: Schaffung grundlegender Regulierung von **Datenintermediären** und sonstiger gemeinsamer Datennutzung; **Datenaltruismus**; Erleichterung des sektorübergreifenden **Datenzugangs und -teilens** – dazu ausführlich unser Newsletter aus dem Januar 2021.

- **Digital Markets Act** (Gesetz über digitale Märkte, kurz DMA) und **Digital Services Act** (Gesetz über digitale Dienste, kurz

DAS) aus Dezember 2020: Schaffung und Schutz des **freien und fairen Wettbewerbs** der digitalen Dienste, Plattformen, Websites etc.; **Sondervorgaben für Gatekeeper** (große Internetplattformen wie Facebook und Amazon) im DMA; Verbesserung der Stellung der Plattformnutzer und -konkurrenten – dazu die Informationswebsites der Kommission zum DSA und DMA.

- **Artificial Intelligence Act** (Künstliche-Intelligenz-Verordnung oder KI-VO): Schaffung eines **Rechtsrahmens für künstliche Intelligenz** unter Berücksichtigung der Risiken und Gefahren; Vorgaben für technische und sonstige Ausgestaltung – dazu ausführlich unser Newsletter aus Mai 2021.

Und damit nicht genug. Parallel zu den laufenden Gesetzgebungsverfahren (zu den jüngsten Entwicklungen zum DMA sogleich) arbeitet die Kommission an weiteren Projekten, die das Digitalpakt ergänzen sollen: Etwa am Entwurf eines weiteren Rechtsakts, der Regelungen für die sektorübergreifende Datenweitergabe in Privatwirtschaft und an staatliche Stellen enthalten soll, sowie an der Schaffung eines unionsweiten digitalen Datenraums für Gesundheitsdaten (European Health Data Space – Informationswebsite der Kommission).

Die unterschiedlichen Gesetzesvorstöße stellen wesentliche Zwischenschritte bei der Umsetzung der Europäischen Datenstrategie der Kommission dar. In dieser formulierte die Kommission ihr Ziel, in den nächsten Jahren eine europäische Datenwirtschaft zu schaffen, in der einerseits das enorme wirtschaftliche und wissenschaftliche Potential von Daten genutzt werden kann, andererseits die Grundrechte und Freiheiten der Bürger sowie die Werte der Europäischen Union hinreichend Beachtung finden. Am Ende der Entwicklung soll ein „echter Binnenmarkt für Daten" stehen, der den Spagat zwischen der Förderung der Datenwirtschaft und dem Schutz der Rechte der Bürger bewältigt.

EDSA: Mangelhafter Datenschutz, fragmentierte Aufsicht und fehlende Kohärenz

Ob der Kommission – und den weiteren am Gesetzgebungsverfahren beteiligten Institutionen, insb. dem Europäischen Parlament – dieser

Spagat mit den bisherigen Verordnungsentwürfen gelungen ist, wird vom EDSA bezweifelt. Dieser nahm bereits dezidiert zu den einzelnen Rechtsakts-Entwürfen Stellung, sah nun aber die Notwendigkeit, einige allgemeine Kritikpunkte zur Umsetzung der Datenstrategie festzuhalten.

In der am 18.11.2021 angenommenen Stellungnahme zum Digital Service Paket und zur Datenstrategie (hier abrufbar in englischer Sprache) benennt der EDSA aus seiner Sicht wiederkehrende Defizite der neuen Vorstöße zur Digitalgesetzgebung: Den mangelhaften Schutz der Grundrechte und Freiheiten der Betroffen, die Gefahr der fragmentierten Aufsicht und das Risiko von Rechtsunsicherheiten und Inkohärenzen.

- Mangelhafter **Grundrechtsschutz** sei unter anderem wegen zu milder Vorschriften gegeben: Nach Auffassung des EDSA sollte etwa die Künstliche-Intelligenz-basierte Kategorisierung von Personen anhand biometrischer Merkmale gänzlich verboten werden und nicht – wie im bisherigen KI-VO-Entwurf – lediglich mit (strengen) Voraussetzungen belegt werden.

- Neben solcher inhaltlicher Kritik bemängelt der EDSA den **fragmentierten Ansatz** der einzelnen Verordnungsentwürfe: Insgesamt werde das Verhältnis zum Datenschutzrecht der DSGVO nicht ausreichend beachtet, obwohl alle vier Verordnungen zumindest in Teilen Wirtschafts- und Lebensbereiche betreffen, in denen personenbezogene Daten verarbeitet werden und die Vorgaben der DSGVO maßgeblich sind. Verweise seien zu allgemein, Datenschutzgrundsätze wie Zweckbindung und Datenminimierung nicht hinreichend beachtet, es fehle an klaren gesetzlichen Erlaubnisgrundlagen für die Verarbeitung personenbezogener Daten und insgesamt werde nicht hinreichend zwischen der Verarbeitung personenbezogener und nicht personenbezogener Daten differenziert. Nach der Auffassung des EDSA birgt dies die Gefahr von Rechtsunsicherheiten, insbesondere, wenn Vorschriften der neuen Verordnungen den Vorgaben der DSGVO (scheinbar) widersprechen.

- Diese Gefahr sieht der EDSA umso mehr bei den geplanten **Aufsichtsmechanismen**. Die Verordnungen enthalten jeweils Vorgaben über die für die Überwachung der Vorschriften

zuständigen Aufsichtsbehörden. In keinem Verordnungsentwurf werden die Datenschutzaufsichtsbehörden mit dieser Aufgabe betraut; die Entwürfe enthalten bisher auch keine Vorschriften zur Einbindung der Datenschutzbehörden, zur Kooperation oder zur Auflösung von Kompetenzkonflikten. Angesichts der überschneidenden Regelungsmaterien prognostiziert der EDSA Kompetenzkonflikte und sieht zudem das Risiko widersprüchlicher oder konkurrierender Behördenentscheidungen gegeben.

In der Konsequenz fordert der EDSA von Kommission und Europäischem Parlament als Gesetzgebungsinstanzen die Überarbeitung der Verordnungsentwürfe: (Mehr) Beachtung sollten dabei die Kohärenz der Entwürfe mit dem gegebenen Datenschutzrecht sowie den wesentlichen Verarbeitungsgrundsätzen der DSGVO finden und Rechtsunsicherheiten und Widersprüche vermieden werden.

Zu guter Letzt

Auch zum Jahresende gab es wieder spannende Bußgeldentscheidungen wegen Datenschutzverstößen. Vier bemerkenswerte Entscheidungen haben wir nachfolgend für Sie zusammengestellt. Auffällig ist dabei, dass drei der vier Bußgelder unter anderem wegen unzureichender technisch-organisatorischer Maßnahmen zur Sicherung personenbezogener Daten verhängt wurden. Dies spiegelt den wachsenden Fokus, den Aufsichtsbehörden auf diesen Aspekt des Datenschutzrechts legen, wider. Thematisch passend erörtern wir in Beitrag 2, ob ein Verzicht auf die Einhaltung von Sicherheitsstandards möglich ist.

- **UK: Bußgeld wegen Veröffentlichung von Postanschriften durch das britische Cabinet Office**

Die britische Datenschutzbehörde (ICO) verhängte eine Geldstrafe in Höhe von rund 585.000 Euro (500.000 GBP) gegen das britische Cabinet Office wegen eines Verstoßes gegen Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 DSGVO, da dieses versehentlich die Ehrungsliste für das Jahr 2020 samt Postanschrift der Empfänger der Ehrungen auf der Internetseite veröffentlichte. Zum Zeitpunkt der Löschung der Datei wurde diese bereits knapp 3.000 mal aufgerufen.

Das Cabinet Office bestätigte, dass es an einem schriftlichen Verfahren fehlte, um Dokumente mit personenbezogenen Daten vor ihrer Veröffentlichung zu genehmigen und sicherzustellen, dass der Inhalt in geeigneter Weise geschwärzt wurde. Aufgrund dessen vertrat das ICO die Auffassung, dass das Cabinet Office auch gegen Art. 32 Abs. 1 DSGVO verstoßen hatte: Es fehlten geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus.

- **Litauen: Bußgeld in Höhe von 110.000 Euro**

Die litauische Datenschutzbehörde (ADA) verhängte gegen eine Autovermietung eine Geldstrafe in Höhe von 110.000 Euro nach einer Datenpanne, die durch unzureichende technisch-organisatorische Maßnahmen zur Sicherung der zu verarbeitenden personenbezogenen Daten verursacht wurde. Personenbezogene Daten von Automietern wurden aus einer ungeschützten Datenbank-Backup-Datei (DB-Datei) abgerufen, enthalten waren u.a. Name, Adresse, Telefonnummer, E-Mail-Adresse, persönliche Identifikationsnummer, Führerscheinnummer, Art der

Zahlungskarte und die letzten vier Ziffern der Nummer, das Ablaufdatum der Zahlungskarte und die Benutzerkennung.

Die Datenschutzbehörde stellte fest, dass eine Reihe von organisatorischen und technischen Sicherheitsmaßnahmen fehlte: Es gab weder eine zuständige Person, die für das Sicherheits- und Risikomanagement verantwortlich war, noch wurden Protokolle über den Zugriff auf die DB-Datei geführt. Die DB-Datei wurde zudem unverschlüsselt gespeichert und lediglich mit schwach verschlüsselten Passwörtern gesichert, die für Personen mit technischen Kenntnissen leicht abrufbar waren.

- **Schweden: Göteborger Berufungsgericht bestätigte Bußgeld gegen Google über 4.800.000 Euro**

Ein Bußgeld in Höhe von rund 5 Mio. Euro gegen Google wegen Verletzung von Löschpflichten nach Art. 17 DSGVO ist vom Göteborger Berufungsgericht bestätigt worden: Das Unternehmen hat Webmaster nicht über die Löschung von Suchergebnissen informiert und nach Ansicht des Gerichts über einen langen Zeitraum die Stellungnahme der Artikel-29-Arbeitsgruppe zum Recht auf Löschung in Suchmaschinen systematisch ignoriert.

- **Frankreich: 400.000 Euro Bußgeld für das staatliche Verkehrsunternehmen „RATP“**

Im Mai 2020 ging bei der französischen Datenschutzbehörde (CNIL) eine Beschwerde mehrerer Gewerkschaften ein, welche die Erhebung und Speicherung von Daten über die Anzahl der Streiktage von Bediensteten des staatlichen Verkehrsunternehmens „RATP“ zum Gegenstand hatte. Die von der CNIL durchgeführte Untersuchung bestätigte, dass diese Praxis in mindestens drei Busbetrieben der RATP praktiziert wurde. Im Zusammenhang der Untersuchung wurden darüber hinaus noch weitere Verstöße gegen die Speicherbegrenzung und die Datensicherheit festgestellt. Die CNIL verhängte aufgrund dessen ein Bußgeld in Höhe von 400.000 Euro gegen RATP.

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