LOSCHELDER

Newsletter Datenschutzrecht
September 2024

Sehr geehrte Damen und Herren,

der Datenschutz bleibt spannend – Neuigkeiten und Bemerkenswertes gibt es immer wieder: Wir beginnen mit einem Blick in die Rechtsprechung, die sich in interessanten Entscheidungen mit der Videoüberwachung eines öffentlichen Parks und der Einwilligung in die Verwendung von Cookies beschäftigt hat.

Mit Cookies beschäftigt sich auch die nun vorliegende „Einwilligungsverwaltungsverordnung" und Einfluss auf die Websitegestaltung hat zudem das Barrierefreiheitsstärkungsgesetz: Hier läuft der Countdown, bis Juni 2025 müssen die adressierten Websites barrierefrei gestaltet sein. Außerdem beabsichtigt die EU anhand einer Verordnung die Durchsetzung datenschutzrechtlicher Pflichten in der EU einheitlicher zu gestalten.

Nach Rechtsprechung und Verordnungs- bzw. Gesetzgebung geht der Blick dann zu den Datenschutzaufsichtsbehörden, die sich in einem interessanten Statement zur Verarbeitung personenbezogener Daten im Asset Deal geäußert und ihren alten Beschluss dazu aktualisiert haben.

Neben all dem noch ein Reminder: Das Gesetzgebungsverfahren zum NIS-2-Umsetzungsgesetz geht weiter, seit dem 16.08.2024 im parlamentarischen Verfahren (BR-Drs. 380/24). IT-Sicherheitsanforderungen werden darin ausgeweitet und betreffen einen deutlich größeren Kreis an Unternehmen. Wir geben Ihnen in unserem nächsten Lunch@Loschelder-Webinar am Donnerstag einen Überblick, welche Unternehmen von dem neuen IT-Sicherheitsrecht adressiert werden und was es bei Betroffenheit zu tun gibt. Kurzentschlossene können sich gerne noch anmelden. Wir freuen uns sehr über Ihr Interesse!

Kommt jetzt die Cybersecurity-Pflicht für alle? Wen betrifft das neue IT-Sicherheitsrecht? Und was muss getan werden?

Donnerstag, den 19. September 2024 - 12.00 bis 12.45 Uhr

Ihre Referenten: Dr. Kristina Schreiber / Dennis Pethke, LL.M. (Stellenbosch)

Alle Webinare bieten wir kostenfrei an und freuen uns über Ihre Anmeldung unter webinare@loschelder.de. Das Webinar findet über Teams statt, der Einladungslink wird rechtzeitig vor der Veranstaltung bereitgestellt.

Selbstverständlich unterstützen wir Sie bei Bedarf auch, wie viele andere unserer Mandanten, bei einer umfassenden Betroffenheitsanalyse mit gutachterlicher Einschätzung oder auch lediglich telefonischem Brainstorming – ganz, wie Sie dies wünschen!

Inhalt

BVerwG: Unterlassungsklage gegen kommunale Videoüberwachung nicht durch DSGVO gesperrt

Gegen eine rechtswidrige Videoüberwachung öffentlicher Plätze kann geklagt werden. Das BVerwG entschied, dass die DSGVO einer Unterlassungsklage nicht entgegensteht, wenn die Überwachung zur Erfüllung öffentlicher Aufgaben, wie in diesem Fall der Bekämpfung von Kriminalität, erfolgt.

Vor dem Bundesverwaltungsgericht ging es kürzlich um Rechtsschutz gegen eine durch die Stadt veranlasste Videoüberwachung (BVerwG, Beschluss vom 02.05.2024 – 6 B 66.23). Hintergrund des Verfahrens ist eine durch die Stadt betriebene Videoüberwachung des öffentlich zugänglichen „Klostergartens“ in Passau. Dadurch sollten kriminelle Aktivitäten im genannten Park bekämpft werden. Ein Passauer Bürger verlangte von der Stadt die Unterlassung der Videoüberwachung und Aufzeichnung von Videos seiner Person. Er sah sich in seinem Recht auf informationelle Selbstbestimmung verletzt und machte einen öffentlich-rechtlichen Unterlassungsanspruch geltend.

VG hielt Klage für unzulässig

In erster Instanz wurde die Klage vom Verwaltungsgericht Regensburg als unzulässig abgewiesen (VG Regensburg, Gerichtsbescheid vom 06.08.2020 – RN 9 K 19.1061). Das VG hat dies damit begründet, dass die Rechte von Betroffenen gegen eine unzulässige Datenverarbeitung durch einen Verantwortlichen oder Auftragsverarbeiter abschließend in der DSGVO aufgeführt seien. Damit sind z.B. das Auskunfts-, Berichtigungs- oder Löschungsrecht gemeint. Zwar enthält die DSGVO ein „Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter“ (Art. 79 DSGVO). Dieses beziehe sich aber lediglich auf diese in der DSGVO genannten Betroffenenrechte. Weitere gerichtliche Rechtsbehelfe – wie die Unterlassungsklage nach § 1004 BGB – seien durch Art. 79 DSGVO ausgeschlossen.

BVerwG lässt Unterlassungsklage zu

Dem hat schon der Bayerische Verwaltungsgerichtshof nach der Berufung des Klägers widersprochen (BayVGH, Urteil vom 30.05.2023 – 5 BV 20.2104). Die Unterlassungsklage sei zulässig. Das BVerwG bestätigte den BayVGH im Mai 2024. Art. 79 Abs. 1 DSGVO stehe der

Geltendmachung eines Unterlassungsanspruchs gegen die kommunale Videoüberwachung aus § 1004 Abs. 1 S. 2 BGB i.V.m. dem Grundrecht auf informationelle Selbstbestimmung nicht entgegen.

Grund dafür sei hier die Rechtsgrundlage für diese Videoüberwachung: Die DSGVO überlasst es nämlich den Mitgliedstaaten, festzulegen, wann eine Datenverarbeitung (u.a. durch Videoüberwachung) zur Wahrnehmung öffentlicher Aufgaben rechtmäßig ist. Dies wurde im Bayerischen Datenschutzgesetz geregelt, worauf sich die Stadt für die Überwachung im „Klostergarten“ gestützt hat (Art. 24 BayDSG). Die Zulässigkeit der Videoüberwachung ist hiernach zu beurteilen – und deshalb auch ein etwaiger Anspruch auf deren Unterlassung. Die DSGVO kann in diesem Fall einer Unterlassungsklage, die sich auf außerhalb der DSGVO geregelte Ansprüche stützt, nicht entgegenstehen.

Neues zu Cookies: OLG-Urteil und Cookie-Verordnung

Mit der Einwilligung in die Verwendung von Cookies setzte sich das OLG Frankfurt auseinander. Nach Ansicht des Gerichts trifft die Pflicht, eine Einwilligung einzuholen, nicht nur Website-Betreiber, sondern auch Diensteanbieter, die Cookies für andere setzen und verwalten. Die bloße Vereinbarung, dass der jeweilige Website-Betreiber verpflichtet ist, eine Einwilligung der Nutzer einzuholen, genüge nicht. Ob dies auch in Zukunft noch relevant ist, wird sich zeigen: Seit Anfang September liegt die Einwilligungsverordnung auf Basis des § 26 TDDDG vor, die die sog. „PIMS" – also Masken zur einheitlichen Einwilligungsverwaltung – stützen und so die Cookie-Banner auf jeder einzelnen Website obsolet machen soll.

„Diese Website verwendet Cookies" – diesen Satz liest man beinahe täglich, woraufhin in der Regel Einwilligungsmöglichkeiten in diese Cookies angeboten werden. Dass diese Einwilligung nicht nur für die Betreiber der Websites essenziell ist, die sog. Publisher, betonte das Oberlandesgericht (OLG) Frankfurt in einem Urteil vom 27.06.2024 (6 U 192/23).

Worum es beim OLG ging

Betreiber von Websites können Tools für eine bessere Vermarktung, bessere Werbemaßnahmen implementieren, beispielsweise Microsoft Advertising. Dadurch werden dann Cookies und andere Tags auf den Endgeräten ihrer Besucher gespeichert. Diese Tags ermöglichen u.a. eine Wiedererkennung der Besucher, um diesen auf Sozialen Medien oder anderweitig das Produkt erneut anzuzeigen o.ä.. Dafür werden in den Tags verschiedenste Informationen über die Online-Aktivität von Usern, wie Anmeldeinformationen, Informationen über angesehene Produkte oder Eingaben in Suchmaschinen erfasst. Durch die Analyse dieser Daten können die Website-Betreiber gezielt Anzeigen bei den Website-Besuchern schalten und den Erfolg von Werbekampagnen messen. Damit diese Technologie funktioniert, stellt etwa Microsoft Advertising als ein Angebot Website-Betreibern einen Programmcode zur Verfügung, der in den Websites eingebunden werden muss.

Die Speicherung von Informationen in der Endeinrichtung des Endnutzers – also etwa der Einsatz von Cookies und vergleichbaren Tags – ist jedoch nach § 25 TDDDG (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, vormals: TTDSG) nur eingeschränkt

zulässig: Wenn der Zugriff nicht nach § 25 Abs. 2 TDDDG erforderlich ist, insbesondere für die Bereitstellung des angefragten Dienstes, muss der Endnutzer zuvor „auf Grundlage von klaren und umfassenden Informationen eingewilligt“ haben. Werbemaßnahmen sind danach regelmäßig nur mit Einwilligung zulässig. Die Voraussetzungen an Information und Ausgestaltung der Einwilligung richten sich nach der DSGVO, auf die § 25 TDDDG dafür verweist.

Die Klägerin warf Microsoft Advertising im vorliegenden Verfahren vor, entgegen der rechtlichen Vorgabe Cookies bei ihr eingesetzt zu haben, ohne dass sie eingewilligt hat.

Microsoft wurde auf Antrag der Klägerin zunächst untersagt, „ohne informierte Einwilligung der Antragstellerin auf deren Endeinrichtungen wie PC, Tablet, Laptop oder Telefon Cookies und ähnliche Technologien einzusetzen, […] um das Verhalten der Antragstellerin im Internet zu werblichen Zwecken zu verfolgen bzw. verfolgen zu lassen“. Diese einstweilige Verfügung wurde anschließend durch das Landgericht wieder aufgehoben. Die Erfüllung der Verfügung hätte einen zu hohen zeitlichen und finanziellen Aufwand erfordert, der außer Verhältnis zu den Interessen der Antragstellerin gestanden hätte. Vielmehr hätte diese selbst das Speichern und Auslesen von Cookies im Browser blockieren können. Dagegen legte die Klägerin Berufung beim OLG Frankfurt ein. Das Gericht gab der Klägerin in zweiter Instanz Recht und bestätigte die einstweilige Verfügung.

Die Begründung des OLG oder warum der Nutzer nicht selber blocken muss

Die Klägerin hat nach Ansicht der OLG Frankfurt einen Anspruch auf Unterlassung des weiteren Einsatzes von Cookies auf ihren Endgeräten ohne erteilte Einwilligung (§§ 823 Abs. 2, 1004 BGB i.V.m. § 25 TDDDG). Denn § 25 TDDDG verpflichte nicht nur Website-Betreiber an sich. Vielmehr sei Microsoft ebenso verpflichtet, Einwilligungen in Cookies einzuholen: Laut dem OLG Frankfurt adressiert die Norm nicht nur Website-Betreiber, sondern „jedermann“, der im Sinne der Norm Cookies speichert oder darauf zugreift, um diese auszuwerten. Microsoft Advertising verpflichtet zwar die Website-Betreiber in ihren AGBs dazu, die erforderliche Einwilligung der Website-Nutzer einzuholen. Das reiche jedoch noch nicht aus, um der gesetzlichen Vorgabe nachzukommen. Vielmehr hätte die Beklagte sicherstellen müssen, dass ihr die Einwilligung des Endnutzers durch den Website-Betreiber übermittelt wird, bevor sie

die Cookies auf dem Gerät der Endnutzerin gesetzt hat. Ein solches Vorgehen wäre auch technisch und rechtlich möglich gewesen. Etwa unter dem TCF des IAB Europe ist es üblich, diese Einwilligungen im Rahmen des sog. Consent String allen Akteuren zu übermitteln. Durch das Unterlassen dieser pflichtgemäßen Handlung habe Microsoft Advertising selbst gegen § 25 TDDDG verstoßen.

Einwilligung „is key"

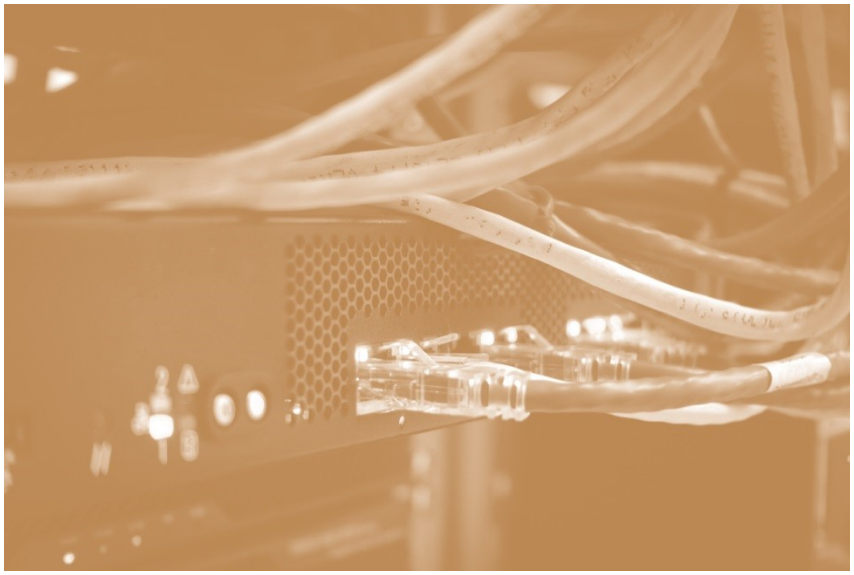
Wer eine Website betreibt und auf Endgeräten der Website-Besucher Cookies platziert, muss deren Einwilligung für die Speicherung von und den Zugriff auf gespeicherte Informationen einholen. Wer Werbe- und Analysedienste durch den Einsatz von Cookies auf Websites von Dritten anbietet, hat sicherzustellen, dass die Website-Betreiber ordnungsgemäße Einwilligungen der Website-Besucher einholen und diese übermitteln.

Das Urteil verdeutlicht die Wichtigkeit der datenschutzrechtlichen Einwilligung bei der Speicherung von Cookies und entsprechenden Tags, die von allen beteiligten Akteuren sicherzustellen ist. Website-Besucher müssen vor einem Kontrollverlust über die Weitergabe ihrer Daten geschützt sein.

Und gibt es künftig dann zentrale Einwilligungsverwaltungssysteme?

Werden die Cookie-Banner auf den Websites also bald noch umfangreicher? Die neue BfDI will dem ausweislich eines aktuellen Interviews in der FAZ ebenso gegensteuern, wie die seit Anfang September veröffentlichte „Verordnung nach § 26 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und zur Änderung der Besonderen Gebührenverordnung Telekommunikation", die nur noch auf die Zustimmung des Bundestages wartet (BT-Drs. 20/12718). Der neuen BfDI sind die „vielen Einverständniserklärungen im Internet … ein Dorn im Auge". Abhilfe schaffen könnten hier sog. „PIMS", Einwilligungsverwaltungssysteme nach § 26 TDDDG, auf denen Nutzer an zentraler Stelle ihre Präferenzen hinterlegen können, die von den Websites dann entsprechend zu berücksichtigen sind, beispielsweise eine generelle Einwilligung in den Einsatz von Analysetools, aber die Verweigerung der Einwilligung in Werbetracking durch Meta und TikTok. Die Gestaltungsoptionen sind vielfältig.

Wer diese PIMS bereitstellen möchte, hat nun mit der neuen Verordnung den entsprechenden Rahmen. Ob dieser aber so gestaltet ist, dass der Markt tatsächlich nutzerfreundliche PIMS bereitstellen wird, ist fraglich: Artikel 1 der oben genannten Verordnung enthält die sog. Einwilligungsverwaltungsverordnung (EinwV) als zentrales Element. Diese EinwV enthält umfangreiche Anforderungen an „anerkannte Dienste“ bei begrenzter Refinanzierungsmöglichkeit. Wird ein anerkannter Dienst von Endnutzern eingesetzt, sichern §§ 17 ff., dass die jeweils getroffenen Einstellungen auch möglichst umfassend berücksichtigt werden.



Barrierefreie Websites: Bald auch für private Unternehmen im E-Commerce Pflicht

Mit dem Barrierefreiheitsstärkungsgesetz werden Anforderungen an die Barrierefreiheit im Internet festgelegt. Websites und Apps sind nicht mehr nur dann betroffen, wenn sie von der öffentlichen Hand betrieben werden, sondern auch, wenn sie von privaten Unternehmen stammen. Diese müssen Maßnahmen treffen, um ihr Online-Angebot ab Juni 2025 so zu gestalten, dass es für Menschen mit Behinderung „ohne fremde Hilfe auffindbar, zugänglich und nutzbar“ ist. Nachfolgend fassen wir zusammen, was darunter genau zu verstehen ist.

Barrierefreiheit wird zukünftig auch für bestimmte Websites, Produkte und Dienste von privaten Unternehmen verpflichtend. Bisher betrafen Pflichten wie große Schrift, Vorlesefunktion und einfache

Sprache lediglich Websites und Apps der öffentlichen Hand. Das ändert sich mit dem Barrierefreiheitsstärkungsgesetz (BFSG) und der zugehörigen Umsetzungsverordnung (BFSGV), die ab dem 28. Juni 2025 in Kraft treten.

Breiter Anwendungsbereich

Das BFSG gilt für alle Unternehmen, die ihre Angebote Verbrauchern online anbieten und so „Dienstleistungen im elektronischen Geschäftsverkehr" anbieten. Diese müssen barrierefrei gestaltet sein, einschließlich der Websites, über die die Dienstleistungen angeboten werden. Das sind z.B. Betreiber von Online-Shops aber auch alle anderen digitalen Möglichkeiten, Verbraucherverträge direkt online abzuschließen (der digitale Fitnessstudiovertrag, direkt am Bildschirm per Klick geschlossen, das neue Paar Schuhe oder der Musikdownload…). Dieser breite Anwendungsbereich wird manches Mal übersehen, da das BFSG zunächst Unternehmen aus bestimmten Sektoren anspricht, wie Personenbeförderungsunternehmen oder Telekommunikationsanbieter (§ 1 Abs. 3 BFSG).

Aber aufgepasst: Wann immer Verbraucher direkt online („elektronisch") einen Vertrag abschließen können, muss dieser Bereich ab Sommer 2025 barrierefrei gestaltet sein! Denn das BFSG adressiert allgemein Websites, die „Dienstleistungen im elektronischen Geschäftsverkehr" anbieten, also insbesondere den Vertragsschluss online ermöglichen. Das Gesetz gilt daneben auch für Hardware, für Universalrechner und zugehörige Betriebssysteme, Smartphones, Tablets, internetfähige Fernseher, E-Books und andere Verbraucherendgeräte mit interaktivem Leistungsumfang.

Anforderungen aus Umsetzungsverordnung

Wie die geforderte Barrierefreiheit ausgestaltet sein muss, ergibt sich aus der Umsetzungsverordnung. Websites müssen „auf konsistente und angemessene Weise wahrnehmbar, bedienbar, verständlich und robust gestaltet werden". Dazu sind beispielsweise eine ausreichend große Schrift, Farbkontraste und einfache Navigationsmöglichkeiten erforderlich, die Sprache muss einfach gestaltet sein, Grafiken müssen beschrieben werden, die Texte sollten vorlesbar sein und auf verschiedenen Endgeräten entsprechend darstellbar. Notwendig sind Informationen über die Produkte, auch mit assistiven Technologien wie Screenreadern, die für den Verbraucher auffindbar,

verständlich und wahrnehmbar sind. Die BFSGV schreibt sogar ausreichende Abstände zwischen den Buchstaben, Zeilen und Absätzen vor. Wenn es Unterstützungsdienste wie einen Call-Center gibt, müssen dort Informationen über die Barrierefreiheit erhältlich sein.

Die Vorgaben gehen damit weit ins Detail – gleichzeitig sind sie aber kaum greifbar. Wie groß genau muss die Schrift sein, wann ist die Sprache „einfach"? Wer es genauer wissen will und hier noch konkretere Anhaltspunkte sucht, bekommt diese in der Norm EN 301 549. Nutzerfreundlicher sind die diversen Checks, die online verfügbar sind. Wir empfehlen hier die öffentlichen Angebote, die im Streitfall besser verwertbar sind.

DSGVO-Durchsetzung in der EU soll einheitlicher werden

Zu viele verschiedene Verfahrensregeln der Mitgliedstaaten stehen einem einheitlich durchgesetzten Datenschutz in der EU entgegen. Zur Verbesserung der Durchsetzung der DSGVO schlug die EU Kommission deshalb eine Verfahrensverordnung vor. Vorgaben zum Beschwerdeverfahren und zur Zusammenarbeit der Datenschutzaufsichtsbehörden stehen hier im Mittelpunkt. Im Juni hat nun auch der Rat seine Position geäußert.

Die EU-Kommission hat im Juli 2023 einen Vorschlag für eine Verfahrensverordnung zur Datenschutz-Grundverordnung (DSGVO) vorgelegt. Sie beinhaltet zusätzliche Verfahrensregeln mit dem

Zweck, eine einheitlichere europaweite Durchsetzung der DSGVO sicherzustellen.

Die DSGVO wurde 2018 mit dem Ziel erlassen, den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten. Eine wirksame Durchsetzung der enthaltenen Vorgaben ist dafür unerlässlich. Dazu haben die Mitgliedstaaten jeweils Aufsichtsbehörden benannt – in Deutschland den Bundes- bzw. die Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Sie haben ihre eigenen Zuständigkeitsbereiche und sorgen darin für die wirksame DSGVO-Durchsetzung. Wenn bei Datenschutzverletzungen Beteiligte aus verschiedenen EU-Mitgliedstaaten involviert sind, wird die Durchsetzung schon schwieriger. Zwar gibt es das Gebot zur Zusammenarbeit und Kohärenz (Art. 51 Abs. 2 DSGVO), wonach die nationalen Datenschutzaufsichtsbehörden innerhalb der EU ein einheitliches Datenschutzniveau sicherstellen sollen. Die nationalen Verfahrensregeln, die von den nationalen Behörden anzuwenden sind, unterscheiden sich allerdings zu sehr, als dass diese Zusammenarbeit reibungslos und wirksam funktionieren kann.

Eine europäische Verfahrensverordnung soll diese Problematik nun beheben. Dazu sieht der Verordnungsvorschlag unter anderem Folgendes vor:

- Ein **vereinheitlichtes Beschwerdeformular** für und die **einheitliche Bearbeitung und Untersuchung** von Beschwerden bei Aufsichtsbehörden mit grenzüberschreitendem Bezug.

- Bei der Zusammenarbeit mehrerer Datenschutzbehörden soll eine rechtzeitige Einigung zwischen diesen durch **frühzeitigeren Informationsaustausch** erleichtert werden, um die formelle Streitbeilegung durch den Europäischen Datenschutzausschuss (EDSA) zu vermeiden.

- Das Recht auf **Anhörung** der von der Untersuchung betroffenen Parteien in wichtigen Phasen des Beschwerdeverfahrens.

Der Vorschlag wurde in Teilen positiv aufgenommen, in einigen Punkten aber auch kritisiert. Er sei zum Teil noch zu lückenhaft und paraphrasiere stellenweise lediglich die DSGVO. Außerdem wurde bemängelt, dass der Vorschlag erst gegen Ende der Legislaturperiode aufkam und eine Fortsetzung des Vorhabens von einem Beschluss im

Parlament abhängt. Trotz des Wechsels der Legislaturperiode wird das Vorhaben vom europäischen Gesetzgeber wohl weiterverfolgt werden. Das EU Parlament beschloss im April 2024 Änderungen am Gesetzesvorschlag. Der Rat setzte sich ebenfalls mit dem Vorschlag auseinander und veröffentlichte im vergangenen Juni seine geänderte Version. Damit bewegt sich die Verordnung auf die Zielgerade. Über die weiteren Entwicklungen halten wir Sie natürlich auf dem Laufenden.

DSK: Neues zur Übertragung personenbezogener Daten beim Asset Deal

Unternehmenskäufe bringen regelmäßig eine Vielzahl datenschutzrechtlicher Fragen mit sich. Eine zentrale Frage ist dabei, ob und wann die Übermittlung personenbezogener Daten im Rahmen des Asset Deals zulässig ist. Die Datenschutzkonferenz hat sich in einem Beschluss vom 11. September 2024 erneut damit beschäftigt und ihren Standpunkt aus Mai 2019 überarbeitet und differenziert. Aus dem neuen Beschluss ergeben sich wichtige Leitlinien für die Praxis.

Beim Asset Deal als Form des Unternehmenskaufs werden – anders, als im Fall eines Share Deals – (einzelne oder alle) Vermögenswerte eines Unternehmens auf ein anderes übertragen. Zu diesen Vermögenswerten zählen in aller Regel auch Daten über Kunden, Lieferanten und Beschäftigte. Damit werden auch personenbezogene Daten übertragen, die erlaubnispflichtig sind.

Wann diese Übertragung datenschutzrechtlich zulässig ist, thematisierte die Datenschutzkonferenz (DSK) bereits in einem Beschluss aus 2019. Dieser Beschluss aus dem Jahr 2019 differenzierte in erster Linie zwischen laufenden Verträgen und Bestandskunden ohne laufende Verträge. Bei Letzteren sollte es darauf ankommen, ob die letzte Vertragsbeziehung länger als drei Jahre zurückliegt, die Übertragung der Daten „aktiver Kunden" war regelmäßig zur Vertragsfortführung erlaubt.

Nunmehr gibt es einen neuen Beschluss der DSK, der am 11.09.2024 veröffentlicht wurde. Dieser neue Beschluss unterscheidet nun zudem nach dem Status des Asset Deals und erst darauf aufbauend der jeweiligen Kundenkategorie, ausgerichtet am Stadium der Vertragsbeziehung mit dem Kunden.

Übermittlung vor Abschluss des Asset Deals (Due Diligence)

Vor Abschluss des Asset Deals ist die Übermittlung nach Position der DSK grundsätzlich unzulässig und lediglich ausnahmsweise zulässig im Falle einer freiwilligen Einwilligung der betroffenen Personen oder – im Zuge bereits fortgeschrittener Übernahmeverhandlungen – aufgrund eines berechtigten Interesses gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Ein berechtigtes Interesse ist jeweils im Einzelfall zu begründen und kann z.B. für Informationen über Hauptvertragspartnerinnen und -partner, Personal mit Führungsverantwortung und/oder für das Geschäft zentralen Kompetenzen bestehen. Dies betrifft nicht die Übermittlung sensitiver Daten nach Art. 9 DSGVO.

Übermittlung von Kundendaten im Rahmen des Asset Deals

Unter welchen Voraussetzungen sodann Kundendaten beim abgeschlossenen Asset Deal übertragen werden dürfen, ist differenziert zu betrachten und richtet sich nach dem Stadium des jeweiligen Vertrags mit dem Kunden:

- Vertragsanbahnung: Führt der Kunde die Verhandlungen mit dem Erwerber von sich aus rügelos fort, greift Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Im Übrigen ist die Übermittlung nur zulässig, wenn den berechtigten Interessen des Veräußerers an der Übermittlung keine überwiegenden Interessen der Kunden entgegenstehen, Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Den berechtigten Interessen der Kunden kann nach dem Beschluss

aber durch eine Widerspruchslösung Rechnung getragen werden. Den Kundinnen und Kunden wird dazu die Datenübermittlung an den Erwerber mit einer angemessenen Frist (etwa 6 Wochen) für einen möglichen Widerspruch angekündigt. Hier bleibt die DSK also bei ihrer schon 2019 präferierten Lösung der Ankündigung mit 6-wöchiger-Widerspruchsfrist. Dies umfasst erneut keine sensitiven Daten.

- Laufende vertragliche Beziehungen: Hierunter fallen alle Vertragsverhältnisse, aus denen der Veräußerer noch Verpflichtungen hat bzw. deren Verjährungs- oder Garantiefristen noch nicht abgelaufen sind. Im Falle der Vertragsübernahme sowie der Schuldübernahme (§ 415 Abs. 1 BGB) bedarf es ohnehin der zivilrechtlichen Zustimmung durch den Kunden. Wird diese erteilt, ist die Übermittlung nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO zulässig. Im Fall der bloßen Erfüllungsübernahme kommt es auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO an. Überwiegende Interessen der Kunden werden aber nach Auffassung der DSK hinsichtlich der für die Erfüllung erforderlichen Daten regelmäßig nicht entgegenstehen, da die Kunden vor allem an der Erfüllung interessiert seien und diese durch den Erwerber besser gewährleistet werden könne, als durch den Veräußerer.

- Beendete vertragliche Beziehung: Altdaten dürfen dem Erwerber zur Erfüllung der gesetzlichen Aufbewahrungs-fristen übermittelt werden, aber nur zu diesem Zweck genutzt werden. Dafür ist dann der Abschluss eines Auftragsverarbeitungsvertrags erforderlich und der Erwerber hat die Daten zwingend von den Daten der Kunden mit laufender Vertragsbeziehung zu trennen („Zwei-Schrank-Lösung“). Für jede darüberhinausgehende Verwendung benötigt der Erwerber die Einwilligung.

- Werbung: Soweit Kontaktdaten der Kundinnen und Kunden nach den vorstehenden Kriterien vom Erwerber verarbeitet werden durften, können diese regelmäßig gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO in dem Umfang für Werbezwecke genutzt werden, wie dies auch durch den Veräußerer zulässig gewesen wäre.

- Sonderfälle: Der Beschluss geht auch auf einzelne Kategorien personenbezogener Daten ein. So dürfen Kundendaten besonderer Kategorien (insb. Gesundheitsdaten) nur mit entsprechender Einwilligung übertragen werden.

Übermittlung von Kundendaten als einziges „Asset"

Im Fall des Verkaufs von Kundendatenbanken als losgelöstes „Asset" ist die Datenübermittlung nach Ansicht der DSK grundsätzlich nur nach wirksamer Einwilligung zulässig. Eine eng umgrenzte Ausnahme macht der Beschluss für den Fall, dass Klein- oder Kleinstunternehmen aufgrund der Beendigung ihrer wirtschaftlichen Tätigkeit, ihre Kunden an ein Klein- oder Kleinstunternehmen desselben Wirtschaftszweigs übergeben. Hier könne die einmalige Übermittlung ausschließlich der Postadressen im Wege der Widerspruchslösung realisiert werden. Die Position der DSK ist hier überaus eng.

Übermittlung von Lieferantendaten

Weniger eng sieht die DSK die Übermittlung der Daten von Lieferanten und deren Beschäftigten. Die Übermittlung wird hier regelmäßig nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zulässig sein. Die DSK weist darauf hin, dass die Lieferanten in der Regel sogar ein Interesse an der Fortführung der Geschäftsbeziehung haben werden.

Bedeutung für die Praxis

Für die Praxis ist der Beschluss ein wichtiger Richtungsweiser, wie die Datenschutzaufsichtsbehörden sich positionieren. Er ist differenzierter, dadurch in einigen Punkten aber auch weniger klar anwendbar im Vergleich zum bisherigen Beschluss aus 2019.

Wesentlich ist zudem: Der Beschluss der DSK spiegelt die Rechtsauffassung der Behörden im Sinne einer Mehrheitsmeinung. Er ist kein geltendes Recht und nicht abschließend. Im Einzelfall können auch andere Übermittlungen erlaubt, kürzere Widerspruchsfristen gerechtfertigt und Abweichungen datenschutzrechtskonform möglich sein.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

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

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

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de