LOSCHELDER

Newsletter Datenschutzrecht

September 2023

Sehr geehrte Damen und Herren,

nach der Sommerpause lesen Sie erneut spannende und praxisrelevante Themen rund um Datenschutz und Datenrecht:

Ein Dauerbrenner in der Praxis ist der Umgang mit Kundendaten in Transaktionen. Eine Gerichtsentscheidung aus Österreich gibt hier wertvolle Hinweise auch für die deutsche Anwendungspraxis. Um den Umgang mit Kundendaten dreht sich auch eine praxisrelevante Entscheidung des LG Baden-Baden, die wir ebenfalls für Sie aufbereitet haben.

Weiterhin aktiv bleibt die EU – aus Brüssel kommen neue Vorgaben für die IT-Sicherheit, die der deutsche Gesetzgeber derzeit umsetzt, und auch Neuigkeiten rund um das Datenrecht. Wir geben Ihnen einen konzisen Überblick über die wichtigsten Entwicklungen.

Schließlich sind auch in den letzten Wochen wieder einige kuriose und spannende Bußgeldentscheidungen aus der EU bekannt geworden – unsere ganz subjektive Auswertung der interessantesten Fälle finden Sie wieder in unserem „Zu guter Letzt".

Wir freuen uns über Ihr Interesse!

Inhalt

Kundendaten im Asset und Share Deal: Was ist erlaubt?

Immer wieder werden in Unternehmenstransaktionen auch personenbezogene Daten übertragen. Gerade Kundendaten haben dabei oft sogar einen relevanten Wert. Wie die Übertragung datenschutzkonform erfolgen kann, beschäftigt die Praxis immer wieder. Die deutschen Datenschutzaufsichtsbehörden haben sich dazu ebenso positioniert, wie jetzt auch der oberste Gerichtshof in Österreich (OGH). Wir fassen die in den verschiedenen Transaktionsphasen wichtigsten Eckpunkte zusammen.

Der datenschutzkonforme Umgang mit Kundendaten in Transaktionen ist essentiell: Nur so wird das Asset gesichert und können Kundendaten auch entsprechend gewinnbringend weiter genutzt werden, nur so können Schadensersatzansprüche und Bußgeldrisiken verhindert werden. In den verschiedenen Transaktionsphasen und -arten sind die folgenden Aspekte datenschutzrechtlich zu bedenken:

Due Diligence

Eine umfassende Due Diligence ist im Vorfeld eines Unternehmenskaufs regelmäßig unerlässlich. Bereits bei diesem Schritt der Unternehmenstransaktion wird oftmals die Offenlegung auch personenbezogener Daten von Kaufinteressenten verlangt, um entsprechend aussagekräftige Prüfungen durchführen zu können. Darunter fallen u.U. auch Kundendaten.

Für die datenschutzkonforme Offenlegung personenbezogener Daten im Rahmen der Due Diligence sind insbesondere folgende Eckpunkte entscheidend:

- Anonymisierung: Soweit möglich, müssen personenbezogene Daten derart geschwärzt und verkürzt werden, dass sie für Kaufinteressenten anonym werden. Die Kaufinteressenten können dann nicht nachvollziehen, zu welcher natürlichen Person bestimmte Informationen gehören.

- Erlaubnisgrundlage: Ohne Anonymisierung dürfen personenbezogene Daten nur dann offengelegt werden, wenn eine Erlaubnisgrundlage dies trägt. In der Praxis kommt hier regelmäßig nur das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Betracht. Die Offenlegung muss dann zunächst überhaupt erforderlich sein, um die berechtigten

Interessen an der Unternehmenstransaktion zu befriedigen. Die Erforderlichkeit kann nur in besonderen Konstellationen und fortgeschrittenen Due Diligence Phasen bejaht werden, wenn es tatsächlich auf die Kenntnis einzelner Kunden ankommt. Und auch dann ist des Weiteren noch eine Abwägung der Interessen erforderlich – die Betroffeneninteressen gegen eine Offenlegung dürfen nicht überwiegen. In der Praxis ist das selten erfüllt.

- Betroffeneninformation: Hinzu kommt rein pragmatisch, dass oftmals in dieser Phase weder Verkäufer noch potentieller Käufer die Kunden, deren Daten offengelegt werden, über die Due Diligence informieren möchte. Mit Offenlegung ist eine solche Information aber i.d.R. geboten nach Art. 13, 14 DSGVO, da die personenbezogenen Daten zu einem neuen Zweck („Verkauf" und nicht mehr Abwicklung der Kundenbeziehung) verarbeitet werden. In Ausnahmefällen kann darauf verzichtet werden; in der Praxis sind die Voraussetzungen dafür aber meist nicht erfüllt.

Festzuhalten bleibt danach: In der Due Diligence sind Kundendaten i.d.R. nicht personenbezogen, sondern nur anonymisiert offenzulegen. Eine personenbezogene Offenlegung kommt nur in Ausnahmefällen in Betracht und erfordert dann die Einhaltung einer Reihe datenschutzrechtlicher Sicherungsmaßnahmen, u.a. der Betroffeneninformation.

Share Deal

Bei dieser Variante einer Unternehmenstransaktion werden lediglich die Gesellschaftsanteile an den Erwerber veräußert. Das Unternehmen, die juristische Person, bleibt identisch. Die datenschutzrechtliche Verantwortlichkeit bleibt damit bei ein und demselben Unternehmen, so dass keine datenschutzrechtlich relevante Datenübermittlung stattfindet. Es fehlt an einer Datenübertragung an einen Dritten. Datenschutzrechtlich gibt es für diese Konstellation im Vollzug mithin regelmäßig keine weiteren Herausforderungen.

Datenschutzrechtliche Herausforderungen können sich jedoch dann ergeben, wenn nach einer Transaktion eine Konzernintegration erfolgt und dann auch Mitarbeiter- oder Kundendaten im Konzern bereitgestellt werden sollen. Die DSGVO sieht bekanntlich kein

Konzernprivileg vor, so dass für eine gemeinsame Datennutzung oder eine Datenübermittlung im Konzern eine Erlaubnisgrundlage nebst Betroffeneninformation erforderlich ist. In der Praxis ist oftmals eine frühzeitige Betroffeneninformation essentiell, um eine „Erwartungshaltung" i.S.d. Erwägungsgrundes 47 DSGVO zu begründen, dass aufgrund der neuen Strukturen personenbezogene Daten nun auch im Konzern verarbeitet werden. Empfehlenswert sind zudem meist konzerninterne Datenschutzvereinbarungen, Data Processing Agreements, die diesen Datenverbund abbilden, sei es über Auftragsverarbeitungsverhältnisse, eine gemeinsame Verantwortlichkeit oder auch trennscharfe Abgrenzungen der Verantwortungsbereiche.

Asset Deal

Werden im Rahmen eines Asset Deals lediglich einzelne Vermögensgegenstände eines Unternehmens veräußert, kommt das Käuferunternehmen als neuer Rechtsträger ins Spiel. Ein solches Asset können auch die Kundendaten sein.

Sollen Kundendaten auf einen neuen Rechtsträger übertragen werden, wechselt der datenschutzrechtlich Verantwortliche. Die personenbezogenen Daten werden an einen Dritten übertragen.

Eine solche Datenübertragung ist erlaubnispflichtig: Als Rechtsgrundlage für die Übertragung kommt zunächst eine Einwilligung eines jeden einzelnen Kunden in die Datenübermittlung in Betracht. Die Einwilligung von aktiven Bestandskunden mit laufenden Verträgen in den Übergang ihrer Daten auf den Erwerber kann auch in der zivilrechtlichen Zustimmung zum Vertragsübergang (§ 415 BGB) gesehen werden. Wie der OGH Österreich kürzlich in einem Beschluss festhielt, ist von einer wirksamen Einwilligung zudem schon dann auszugehen, wenn Kunden beim Bezug eines Newsletters zustimmen, dass im Falle des Verkaufs des Unternehmens ihre Daten an den Käufer übertragen werden. Das gilt aber nur, wenn die Kundendaten auch für dieselben Zwecke weiterverwendet werden, für die sie erhoben wurden. Nutzt der Erwerber also die Daten, um weiterhin Werbung und Newsletter an die Kunden zu verschicken, sei es entbehrlich, eine neue Einwilligung einzuholen. Auch bestehe keine zusätzliche Informationspflicht gem. Art. 14 DSGVO gegenüber den betroffenen Personen. Die Daten wurden von der erworbenen Gesellschaft bei

den Kunden und nicht bei einer anderen Person (dem Verkäufer) erhoben.

In der Praxis ist eine Einwilligung allerdings trotz der weiten Auslegung durch den OGH Österreich oft nicht der bevorzugte Weg: Zum Transaktionszeitpunkt ist dann oft nicht sicher, welcher Kunde zustimmt. Der Wert des Assets ist nicht bestimmbar; es besteht ein erhebliches Risiko, dass nur wenige Kunden einwilligen. Die Einwilligung ist in vielen Fällen auch nicht interessensgerecht, wenn der Erwerber etwa bestehende Verträge weiterhin erfüllen will. Anstelle einer Einwilligung können denn auch berechtigte Interessen von Verkäufer und Erwerber eine Rechtsgrundlage zur Übertragung der Kundendaten bieten. Entscheidend ist, dass die gegenläufigen Interessen der Kunden nicht überwiegen. In der Praxis orientiert sich die Bewertung der berechtigten Interessen nach wie vor an den von der Datenschutzkonferenz (DSK) in einem Papier aus 2019 entwickelten Fallgruppen:

- Bestandskunden mit aktiven Verträgen oder letzter Vertragsbeziehung vor weniger als drei Jahren: Daten dürfen aus berechtigten Interessen übermittelt werden, wobei den Kunden eine Widerspruchsmöglichkeit vor der Übermittlung eingeräumt werden muss (i.d.R. mit 6 Wochen Frist).

- Bestandskunden ohne aktiven Vertrag mit letzter Vertragsbeziehung vor mehr als drei Jahren: Daten dürfen übermittelt werden, aber nur, wenn dies zur Erfüllung gesetzlicher Aufbewahrungsfristen erforderlich ist, wobei auch hier ein Widerspruch ermöglicht werden muss.

- Die vorstehenden Kriterien gelten nur für nicht sensible Daten, also u.a. nicht für Gesundheitsdaten. Für diese ist stets eine Einwilligung erforderlich.

In der Praxis empfiehlt sich danach eine frühzeitige Information der Kunden über den bevorstehenden Asset Deal mit Einräumung einer Widerspruchsfrist. Wann noch von aktiven Kunden ausgegangen werden kann und wie lange eine Frist zu gewähren ist, ist eine Frage des Einzelfalls. Die Kriterien der DSK können mit Blick auf das jeweils betroffene Geschäft auch kürzer oder länger gewählt werden, je nach den üblichen Abläufen: Wenn häufig Kunden nach 5 oder 6 Jahren erneute Vertragsbeziehungen aufnehmen, können auch diese noch als aktive Kunden qualifiziert werden. Maßgeblich ist, dass –

im Rahmen der ohnehin zu dokumentierenden Interessensabwägung unter Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO – die gewählten Zeiträume begründet werden.

Das neue IT-Sicherheitsrecht: Was jetzt auf Unternehmen zukommt

Die seit Dezember 2022 in Kraft getretene NIS-2-Richtlinie beinhaltet neue Anforderungen an Cybersicherheit im Unternehmen. Zu ihrer Umsetzung liegt inzwischen ein deutscher Referentenentwurf vor, der Unternehmen erweiterte Pflichten auferlegt. Unternehmen sollten sich angesichts des erheblichen Umsetzungsaufwandes schon früh damit beschäftigen, ob sie adressiert werden und welche Pflichten das neue Gesetz für sie bringen wird. Welche dies sind, zeigen wir Ihnen in diesem Beitrag.

Cyber-Angriffe nehmen zu, eine gute IT-Sicherheit wird immer wichtiger. Dies hat auch die EU erkannt und steuert mit verschiedenen Rechtsakten in diese Richtung. Schon zum Jahreswechsel ist dazu die NIS-2-Richtlinie verabschiedet worden, über die wir in unserer Januar Ausgabe berichteten. Als Richtlinie muss diese vom deutschen Gesetzgeber umgesetzt werden. Seit Juli 2023 liegt nunmehr ein offizieller Referentenentwurf für ein entsprechendes Umsetzungsgesetz vor. Er bringt wesentliche Neuerungen und weitreichende Pflichten für eine Vielzahl von Unternehmen, nicht nur für die bekannten KRITIS-Anlagen. Grund genug, sich schon frühzeitig mit den anstehenden Neuerungen zu beschäftigen:

Erweiterter Adressatenkreis

Wie auch schon bisher werden KRITIS-Unternehmen, also u.a. Unternehmen in der Energiewirtschaft, der Wasserversorgung oder Krankenhäuser, in Sachen IT-Sicherheit reguliert.

Die Umsetzung der NIS-2-Richtlinie wird indes deutlich mehr Unternehmen erfassen als bisher: Neu erfasst sind beispielsweise Unternehmen der chemischen Industrie, des Maschinenbaus, des produzierenden Gewerbes oder auch „digitale Dienste“. Adressiert werden dabei nicht nur große, sondern auch mittlere Unternehmen der einschlägigen Sektoren, also schon solche ab 50 Beschäftigten und einem Jahresumsatz von 10 Mio. Euro.

Welche Pflichten diese Adressaten jeweils genau treffen, ist von ihrer Bedeutung abhängig. Das Umsetzungsgesetz differenziert zwischen „besonders wichtigen“ und „wichtigen Einrichtungen“ (§ 28 BSIG-E).

Schadensprävention

Inhaltlich geht es neben erweiterten Befugnissen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) insbesondere um vielseitige Pflichten der betroffenen Unternehmen.

Insbesondere müssen die Unternehmen umfassende Risikomanagementsysteme etablieren (§ 30 BSIG-E). Dies umfasst technische und organisatorische Maßnahmen zur präventiven Vermeidung von Störungen. Durch diese Risikomanagementmaßnahmen sollen die Auswirkungen etwaiger Sicherheitsvorfälle auf die eigenen und auch auf andere Dienste verhindert bzw. möglichst gering gehalten werden. Zu den Mindestanforderungen zählen zum Beispiel Konzepte zur Risikoanalyse, zur Bewältigung von Sicherheitsvorfällen, das Back-Up Management aber auch die Sicherheit des Personals.

Verantwortung der Leitungsebene

Für die Umsetzung dieser Risikomanagementmaßnahmen soll die Leitungsebene künftig persönlich in Anspruch genommen werden: Geschäftsleiter müssen nach § 38 BSIG-E die vorgesehenen Maßnahmen überwachen und billigen, sonst droht die persönliche Haftung. Um dazu fähig zu sein, werden Schulungen der Leitungsebene, des "Cyber-Vorstands“, zwingend vorgeschrieben.

Was jetzt zu tun ist

Wichtig für Unternehmen ist es – je früher desto besser – zu prüfen, ob sie unter den Anwendungsbereich des Umsetzungsgesetzes der NIS-2-Richtlinie fallen. Wenn sie erstmals vom IT-Sicherheitsrecht erfasst sind, warten erhebliche Umsetzungsanforderungen. Auch wenn die Maßnahmen erst zum Oktober 2024 implementiert sein müssen, sollte ausreichend Zeit eingeplant werden. Mehr Informationen zum neuen IT-Sicherheitsrecht finden Sie auch auf unserem Blog unter dem #cybersecurity.

Der Data Governance Act wird aktiviert: Logos für die Kennzeichnung anerkannter Dienste

Der Data Governance Act gilt ab dem 24.09.2023 und regelt u.a. die Registrierung sog. „datenaltruistischer Organisationen" sowie die Anmeldung von „Anbietern von Datenvermittlungsdiensten". Für beide Einrichtungen soll es künftig einheitliche Logos geben. Diese sind nun von der Kommission vorgestellt worden. Wir geben einen Überblick darüber, was damit bezweckt werden soll und wer ein solches Logo verwenden darf.

Mit dem Data Governance Act (DGA) wurde die erste Säule der EU-Datenstrategie umgesetzt. Seine wesentlichen Regelungen haben wir bereits im Juni 2022 in unserem Newsletter vorgestellt. Als EU-Verordnung gilt der DGA in jedem Mitgliedstaat unmittelbar ab dem 24.09.2023. Einzig diejenigen Einrichtungen, die bereits seit dem 23.06.2022 Datenvermittlungsdienste im Sinne des DGA erbringen, müssen dessen Verpflichtungen erst ab dem 24.09.2025 nachkommen (Art. 38 DGA).

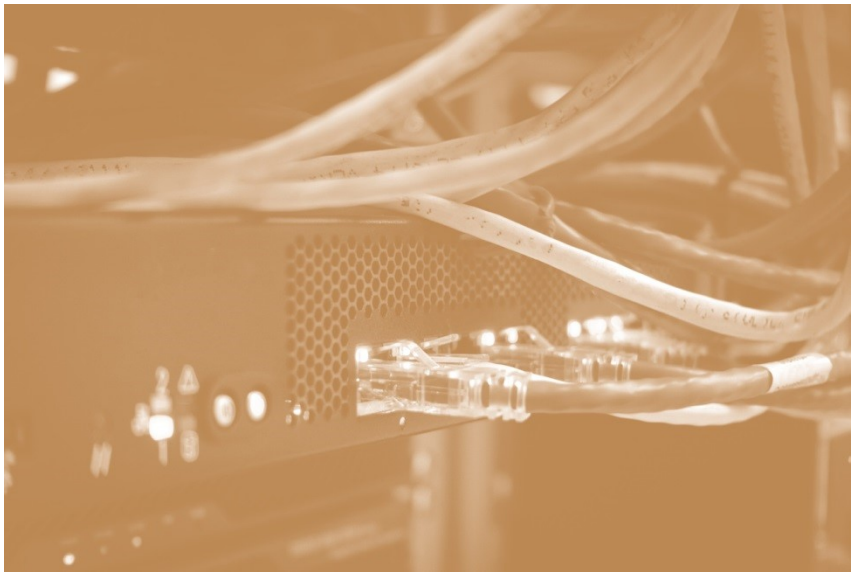
Die EU-Kommission wird im DGA dazu ermächtigt in bestimmten Fällen ergänzende Durchführungsrechtsakte zu erlassen, die eine einheitliche Anwendung des DGA in der EU gewährleisten sollen. Nun hat die Kommission entsprechend der Art. 11 und 17 DGA in einer ersten Durchführungsverordnung Logos für in der Union anerkannte Datenvermittlungsdienste sowie datenaltruistische Organisationen festgelegt. Diese Datenvermittlungsdiente und datenaltruistische Organisationen haben die jeweiligen Logos gut sichtbar zu verwenden, damit leicht erkennbar ist, dass sie offiziell anerkannt sind. Mit den Logos soll Vertrauen in die anerkannten Einrichtungen geschaffen werden, um so das übergeordnete Ziel eines freiwilligen Datenaustauschs zu fördern. Wie diese Logos konkret aussehen, kann im Anhang des Durchführungsrechtsakts eingesehen werden.

Datenvermittlungsdienste im Sinne des DGA meint Dienste, die das Teilen von (personenbezogenen) Daten mit Dritten zur deren weiteren Nutzung dieser Daten fördern sollen. Anerkannt werden solche Datenvermittlungsdienste dann, wenn sie bei der zuständigen Behörde angemeldet sind und die Bedingungen des Art. 12 DGA erfüllen. Darunter fallen datenschutzrechtliche Aspekte aber auch der faire, transparente und nichtdiskriminierende Zugang zu den Diensten.

Datenaltruistische Organisationen können sich im öffentlichen nationalen Register als anerkannt eingetragen lassen. Sie gelten dann als in der Union anerkannt und dürfen das Logo verwenden. Die Anforderungen für die Registrierung sind in Art. 18 DGA festgehalten. Wesentlich ist die Ausübung einer datenaltruistischen Tätigkeit, also das freiwillige Teilen von Daten für Ziele von allgemeinem Interesse (z.B. das Teilen medizinischer Forschungsdaten).

Dass die Logos in Zukunft zur Kennzeichnung von Datenvermittlungsdiensten und datenaltruistischen Organisationen verwendet werden müssen, kann dazu beigetragen Vertrauen in diese Einrichtungen hervorzurufen und die Bereitschaft zum Datenteilen zu fördern. Nur wenn genügend Daten freiwillig geteilt werden, kann das vom Unionsgesetzgeber mit dem DGA verfolgte Ziel eines europäischen Binnenmarkts für Daten auch tatsächlich erreicht werden.

Die Praxis steht aktuell indes noch vor der großen Herausforderung, dass trotz des nahenden Inkrafttretens in Deutschland die für die Anmeldung und Registrierung zu benennenden Behörden noch nicht benannt sind: Es droht damit ein Umsetzungsdefizit.



Neues zum Data Act: Abschluss der Trilog-Verhandlungen

Die zweite Säule der EU-Datenstrategie ist der Data Act. Für die Datenwirtschaft wird dieser deutlich größere Auswirkungen mit sich bringen als der Data Governance Act. Die Trilog-Verhandlungen zum Data Act wurden kürzlich abgeschlossen. Der ursprüngliche Verordnungsentwurf wurde in vielen Teilen durch das Europäische Parlament und den Rat abgeändert. In Arbeit ist nur der finale Text, mit dessen Veröffentlichung im Herbst 2024 zu rechnen ist. Im Folgenden stellen wir die wesentlichen Inhalte des Data Acts dar und geben einen Ausblick auf die zu erwartenden zeitlichen Abläufe.

Im Rahmen der Trilog-Verhandlungen zwischen EU-Kommission, Europäischen Parlament (EP) und Rat konnte Ende Juni dieses Jahrs eine Einigung über den finalen Text des Data Act erzielt werden. Diese „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung", kurz „Datengesetz" oder eben „Data Act" muss nun ausgefertigt und formal verabschiedet werden. Der Data Act wird voraussichtlich im Herbst 2024 im Amtsblatt der EU veröffentlicht und 20 Tage danach in Kraft treten. Zwar ist der finale Verordnungstext noch nicht sicher bekannt, die Änderungsvorschläge von EP und Rat zum ursprünglichen Entwurf sind jedoch bekannt (siehe dazu auch unseren Beitrag von April 2022). Damit wird es nun für die Adressaten des Data Act vorhersehbarer, welche Pflichten sie in Zukunft umzusetzen haben und welche Neuerungen im Zusammenhang mit Datenzugang und -nutzung auf sie zukommen. Auch wird klar, dass die Vorgaben in absehbarer Zeit in Kraft treten werden.

Der Data Act richtet sich an Hersteller und Nutzer vernetzter Produkte und verbundener Dienste. Darunter können Haushaltsgegenstände und Autos aber auch mit Produkten verbundene Software fallen. Cloud-Angebote sind ebenso erfasst wie diverse Apps. Der Data Act bezieht sich dabei sowohl auf personenbezogene als auch auf nicht-personenbezogene Daten, etwa Maschinendaten.

Das übergeordnete Ziel des Data Act ist der Aufbau einer unionsweiten Datenwirtschaft. Das Potenzial einer umfassenden Datennutzung soll zukünftig besser ausgeschöpft werden. Als EU-

Verordnung wird der Data Act unmittelbar in jedem EU-Mitgliedstaat gelten, ohne dass ein nationales Umsetzungsgesetz erforderlich ist.

Wir stellen Ihnen hier die wesentlichen Bausteine des Data Act vor:

Datenzugang und Recht auf Weitergabe

Nutzer erhalten einen Anspruch auf Zugang nutzergenerierter Daten in digitalen Produkten. Dieser Zugang soll möglichst in Echtzeit zur Verfügung gestellt werden. Ob der Nutzer den Zugang selbst nutzt oder aber dies einem Dritten bereitstellt, ist ihm überlassen.

Vor allem die Möglichkeit Dritter, auf Nutzerdaten zuzugreifen, kann zu neuen Innovationen beitragen. Produkteanbieter können mit den Informationen ihre Produkte verbessern oder diese durch weitere Anwendungen oder Supportleistungen ergänzen. In Wettbewerb zum Zugang gewährenden Anbieter dürfen sie aber nicht treten. Dennoch wird bemängelt, dass der Geschäftsgeheimnisschutz unzureichend ist – das Zugangsrecht ist insoweit im ursprünglichen Entwurf zu weit geraten und auch EP und Rat haben hier keine Änderungsvorschläge eingebracht, die einen wirksamen Schutz sicherstellen würden.

Vertragskontrolle: keine missbräuchlichen Klauseln

Verträge dürfen keine missbräuchlichen Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen enthalten. Diese Art AGB-Kontrolle soll verhindern, dass ein erhebliches Ungleichgewicht zwischen den Vertragsparteien entsteht. Das ist z.B. bei einem einseitigen Haftungsausschluss der Fall. Ursprünglich sollten nur KMU geschützt werden – in den Verhandlungen ging die Tendenz aber zu einer Ausweitung auf alle Unternehmen, unabhängig von ihrer Größe.

Bereitstellung von Daten für Behörden

Im Falle einer „außergewöhnlichen Notwendigkeit“ müssen Dateninhaber öffentlichen Stellen Daten bereitstellen. Behörden können also zukünftig bei öffentlichen Notständen oder zu deren Vorbeugung von Herstellern vernetzter Produkte die bei der Nutzung erzeugten und verfügbaren Daten verlangen. Diese Befugnis soll nach Ansicht des EP auf nicht personenbezogene Daten beschränkt werden. Der Rat war entgegengesetzter Meinung. Wie

weit der Anwendungsbereich dieser Regelung sein wird, wird sich somit erst aus dem finalen Text ergeben. Praktisch relevant war dieser – damals noch nicht geregelte – Fall etwa während der Corona-Pandemie, als große Telekommunikationsunternehmen den Behörden anonymisierte Bewegungsdaten zur Verfügung stellten.

Vereinfachter Wechsel zwischen Cloud-Anbietern

Anbieter von Datenverarbeitungsdiensten müssen die Migration zu einem anderen Dienst ermöglichen, ohne technische oder finanzielle Hindernisse. Dieses sog. „Cloud-Switching" soll LockIn-Effekte verringern und den Markt damit stärken. Anbieter von Datenverarbeitungsdiensten müssen in Zukunft den Wechsel zu anderen Anbietern ermöglichen, indem etwaige Hindernisse beseitigt werden. Das können gewerbliche, technische, vertragliche sowie organisatorische Hindernisse sein. Dabei muss gewährleistet werden, dass die Funktionen auch während eines Wechselvorgangs kontinuierlich aufrechterhalten werden. Diese Regelung könnte für KMU und neue Marktteilnehmer sehr belastend wirken. Diesem Aspekt möchte das EP unter anderem damit entgegenwirken, dass Unternehmen nur im Rahmen ihrer Kapazitäten handeln müssen und nur, soweit dies auch wirklich relevant ist für die gewünschte Marktöffnung. Der finale Text bleibt hier mit Spannung abzuwarten. Nach Inkrafttreten beginnt eine Umsetzungsfrist von 18 Monaten zu laufen.

Herausforderungen

Auch wenn die wesentlichen Regelungskomplexe des Data Act damit klar abgesteckt sind, bleiben im Detail etliche Fragen. Für erhebliche Herausforderungen und Unsicherheiten in der Umsetzung werden insbesondere die unklaren Definitionen im Data Act, das nicht konkretisierte Verhältnis zur DSGVO sowie der wohl unzureichende Geschäftsgeheimnisschutz sorgen. All dies könnte dem innovationsfördernden Motiv der Verordnung entgegenstehen.

LG Baden-Baden: Leitlinien für die Verarbeitung von Kundendaten notwendig

Welche Pflichten treffen ein Unternehmen, wenn ein Arbeitnehmer über sein privates Endgerät und die sozialen Medien Kontakt zu einem Kunden aufnimmt? Das LG Baden-Baden beschäftigte sich jüngst mit einem solchen Fall. Wir haben die wichtigsten Eckdaten für Sie aufbereitet.

Die Verarbeitung von Kundendaten im Unternehmen ist ein wesentlicher Bestandteil der unternehmerischen Tätigkeit. Handelt es sich um natürliche Personen, so unterliegen sie als personenbezogene Daten dem Schutz der DSGVO. Das gilt auch, wenn Mitarbeiter eines Unternehmens Kundendaten nutzen, um auf privaten Kommunikationsgeräten mit Kunden zu interagieren, wie das LG Baden-Baden kürzlich entschied.

Die Klägerin hatte bei dem beklagten Unternehmen einen Fernseher sowie eine Wandhalterung erworben, letztere jedoch wieder zurückgegeben. Fälschlicherweise wurde ihr daraufhin der (höhere) Preis des Fernsehers zurück überwiesen. Eine Mitarbeiterin des Unternehmens bemerkte dies und nahm über die sozialen Medien auf privatem Wege Kontakt mit der betroffenen Kundin auf. Sie machte diese auf das Versehen aufmerksam und bat um Rückmeldung. Die Kundin verlangte anschließend vom Unternehmen gem. Art. 15 DSGVO Auskunft darüber, an welche Mitarbeiter ihre Daten übermittelt wurden. Zudem beantragte sie, das Unternehmen dazu zu verurteilen, seinen Mitarbeitenden zu

untersagen, Kundendaten auf privaten Kommunikationsgeräten zu nutzen. Nach Zurückweisung der Klage durch das AG Bühl hat das LG Baden-Baden nun in zweiter Instanz der Berufung der Kundin stattgegeben.

Das datenschutzrechtliche Auskunftsrecht erstreckt sich gem. Art. 15 Abs. 1 lit. c) DSGVO auch auf Empfänger der Daten der betroffenen Person. Empfänger sind dabei alle natürlichen oder juristischen Personen, denen Daten offengelegt werden – grundsätzlich allerdings nicht Arbeitnehmer des Verantwortlichen. Der Europäische Gerichtshof (EuGH) entschied jedoch im Juni 2023, dass dies nur gilt, wenn Arbeitnehmer unter Aufsicht und auf Weisung des Verantwortlichen Kundendaten verarbeiten. Handeln Arbeitnehmer wie im vorliegenden Fall jedoch eigenmächtig und über ihr privates Gerät, ist dies nicht mehr dem Verantwortlichen zuzurechnen. Deshalb ist die Mitarbeiterin als Empfängerin im Rahmen des Auskunftsanspruchs zu benennen. Mit dieser Auskunft wird der Kundin ermöglicht, die Rechtmäßigkeit der Datenverarbeitung zu überprüfen sowie gegebenenfalls bestehende weitere Ansprüche gegen die konkrete Mitarbeiterin geltend zu machen.

Der beantragte Unterlassungsanspruch der Kundin wurde ebenfalls bestätigt. Die vorliegende mehrfache Nutzung von Kundendaten auf privatem Wege stellte ein weisungswidriges Verhalten der Mitarbeiterin dar. Das Unternehmen hat dies als mittelbare Handlungsstörerin zu unterbinden.

Das Urteil des LG Baden-Baden verdeutlicht nochmals die internen Organisationspflichten zur Umsetzung des Datenschutzes: Durch entsprechende Richtlinien ist sicherzustellen, dass der Datenschutz auf allen Ebenen eingehalten wird. Es ist zu regeln, wie personenbezogene Kundendaten verarbeitet werden dürfen.

Zu guter Letzt

Auch in den letzten Wochen gab es spannende Entscheidungen zum Datenschutz und teils erhebliche Bußgelder: Die schwedische Datenschutzbehörde hat nach erfolgreicher Untätigkeitsklage dem bekannten Musikstreamingdienstleister Spotify AB ein Bußgeld auferlegt, die Berliner Datenschutzbehörde bemängelt die fehlende Transparenz einer automatisierten Kreditablehnung und die norwegische Datenschutzbehörde verbietet Facebook und Instagram verhaltensbasierte Werbung zu schalten. Zudem hat die irische Datenschutzbehörde dem Konzern Meta ein Rekordbußgeld in Höhe von 1,2 Milliarden Euro und gegen TikTok in Höhe von 345 Millionen Euro auferlegt.

- **Schweden – Gegen Spotify wurde ein Bußgeld von umgerechnet knapp 5 Millionen EUR verhängt**

Die Schwedische Datenschutzbehörde hat dem Musikstreaminganbieter Spotify AB, dessen Hauptsitz in Schweden ist, ein Bußgeld in Höhe von 58 Millionen schwedischen Kronen auferlegt. Die Datenschutzbehörde wurde tätig, nachdem der Aktivist Max Schrems, der bereits 2019 Beschwerde gegen Spotify einlegte, erfolgreich gegen die Untätigkeit der Datenschutzbehörde klagte. Spotify wird unter anderem vorgeworfen, der Bearbeitung von Auskunftsersuchen nicht ausreichend nachgekommen zu sein. Das Bußgeld ist in Anbetracht des Jahresumsatzes von Spotify moderat – die Datenschutzbehörde hätte ein Bußgeld bis zu 200

Millionen EUR fordern können. Zur Begründung führt sie an, dass die Verstöße wenig schwerwiegend seien.

- **Berlin: Datenschutzbehörde verhängt Bußgeld in Höhe von 300.00 Euro gegen eine Bank wegen mangelnder Transparenz**

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat gegen eine Bank ein Bußgeld in Höhe von 300.000 Euro verhängt. Ein Kunde mit gutem Schufa-Score und hohem Einkommen konnte nicht nachvollziehen, wieso die Bank seinen Antrag auf Kreditvergabe im Rahmen einer automatisierten Entscheidung ablehnte. Auf seine Nachfrage hin gab ihm die Bank nur pauschale Informationen zum Scoring-Verfahren. Nach Beschwerde des Kunden bei der Berliner Datenschutzbehörde verhängt diese gegenüber der Bank das Bußgeld aufgrund eines von ihr gesehenen Verstoßes gegen Art. 22 Abs. 3, Art. 5 Abs. 1 lit. a und Art. 15 Abs. 1 lit. h DSGVO: Die Bank sei ihrer Verpflichtung nicht nachgekommen, die erfolgte automatisierte Entscheidung nachvollziehbar und schlüssig zu begründen.

- **Norwegen: Drei-Monatiges Verbot für Meta, verhaltens-basierte Werbung zu schalten**

Die norwegische Datenschutzbehörde hat in einem Eilverfahren angeordnet, dass Meta auf seinen beiden sozialen Netzwerken Facebook und Instagram keine verhaltensbasierte Werbung mehr anzeigen darf. Die bisherige Art und Weise des Unternehmens, Nutzerdaten für Marketingzwecke zu erheben und zu verwenden, sei rechtswidrig – dies habe auch kürzlich der EuGH in seinem Urteil vom 04.07.2023 bestätigt. Das Verbot gilt vom 04.08. bis zum 03.11.2023, solange nicht die beanstandeten Datenschutzverstöße beseitigt wurden. Sollte Meta gegen das Verbot verstoßen, kann die norwegische Datenschutzbehörde eine Geldstrafe in Höhe von umgerechnet 89.500 Euro pro Tag verhängen. Für den Zeitraum ab November muss dann noch in der Hauptsache entschieden werden.

- **Irland: Datenschutzbehörde verhängt Bußgelder gegen Meta und TikTok**

Die irische Datenschutzbehörde hat ein Rekordbußgeld in Höhe von 1.2 Milliarden EUR gegen Meta verhängt. Auch in diesem Fall hat der Aktivist Max Schrems die Datenschutzbehörde durch eine Beschwerde zum Tätigwerden veranlasst. Anlass für das Bußgeld

war, dass Meta Nutzerdaten an die USA übermittelt habe trotz eines entgegenstehenden Gerichtsurteils. Zudem wurde Meta dazu verpflichtet, zukünftig alle Datentransfers in die USA zu unterbinden. Meta kündigte an, Berufung gegen die Entscheidung einlegen zu wollen.

Am 01.09.2023 folgte sodann ein Bußgeld der irischen Datenschutzbehörde gegen TikTok in Millionenhöhe: 345 Mio. Euro Bußgeld sprach die Behörde wegen Datenschutzverstößen bei den Voreinstellungen und der Altersverifikation aus, u.a. wegen unzulässiger Dark Patterns.

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

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

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

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

Dennis Pethke, LL.M.
+49(0)221 65065-200
dennis.pethke@loschelder.de

Impressum

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

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